RESUMEN – TRABAJO DE GRADO

AUTORES	**EDGAR ANDRES MUÑOZ VILLERO** **LUIS MANUEL PALMERA QUINTERO**
FACULTAD	**INGENIERÍAS**
PLAN DE ESTUDIOS	**ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS.**
DIRECTOR	**ANA MELISA RODRÍGUEZ CHINCHILLA**
TÍTULO DE LA TESIS	**PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION PARA LA EMPRESA FQ TECNOLOGIAS S.A.S, BASADO EN LA NORMA ISO 27001:2013**

RESUMEN
(70 palabras aproximadamente)

ESTE ESTUDIO DOCUMENTA LA PLANEACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN APLICABLE A LA EMPRESA FQ TECNOLOGIAS SEGÚN LA NORMA ISO 27001/2013, RESALTANDO LOS ASPECTOS DONDE ES NECESARIO PONER EN PRACTICA LOS CONTROLES DE SEGURIDAD DE LA INFORMACION EN FUNCIÓN DE LOS RIESGOS QUE EXISTEN Y EL NIVEL DE CONFIDENCIALIDAD QUE SE LE BRINDA A LOS ACTIVOS DE INFORMACIÓN DENTRO DE LA EMPRESA, SE RECOMIENDA LA MANERA MAS EFICIENTE DE EVITAR PERDIDA DE INFORMACION, ROBOS, DAÑOS EN LOS EQUIPOS DE COMPUTO, Y DAÑOS INTENCIONALES O NO INTENCIONALES QUE PUEDAN AFECTAR LA DISPONIBILIDAD, ASI COMO CUMPLIR CON LOS OBJETIVOS PROPUESTOS PARA EL CUMPLIMIENTO DE LOS CONTROLES Y SERVICIOS UTILIZADOS POR LA EMPRESA.

CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM:
121	0	0	1

PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACION PARA LA EMPRESA FQ TECNOLOGIAS S.A.S, BASADO EN LA NORMA ISO 27001:2013

Autores

EDGAR ANDRES MUÑOZ VILLERO

LUIS MANUEL PALMERA QUINTERO

Proyecto Presentado Como Requisito Para Optar Por El Título De Especialista En Auditoria De Sistemas

DIRECTOR:

MSC. ANA MELISSA RODRIGUEZ CHINCHILLA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACIÓN AUDITORIA DE SISTEMA

Ocaña, Colombia **Mayo, de 2019.**

ADVERTENCIA

GLOSARIO

Riesgo: posibilidad de que se produzca un contratiempo, de que alguien o algo sufra perjuicio o daño.

Aceptación del Riesgo: decisión de asumir un riesgo.

Activo: son los bienes, derechos y otros recursos de los que dispone una empresa.

Amenaza: peligro inminente, que surge, de un hecho o acontecimiento que aún no ha sucedido.

Análisis de Riesgo: determina los factores de riesgo que potencialmente tienen efecto en la empresa.

Auditoría: es la revisión de cuentas de una empresa con el objetivo de investigar se están de acuerdo con las disposiciones establecidas.

Confidencialidad: se trata de una propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas.

Seguridad Informática: conjunto de herramientas, procedimientos y estrategias que tienen como objetivo garantizar la integridad, disponibilidad y confidencialidad de la información.

SGSI: para la empresa es el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información.

Integridad de datos: se refiere la correctitud y completitud de la información en una base de datos.

Gestión de Riesgos: es el proceso de identificar, analizar y responder a factores de riesgos a lo largo de la vida en un proyecto.

DEDICATORIA

Dedico este nuevo logro en mi vida al ser que actúa en mi cada día "DIOS", por darme la fuerza, la constancia, la sabiduría y sobre todo por mostrarme que quien trabaja con fe, dedicación y perseverancia puede alcanzar sus objetivos.

A mi madre **ILVA DEL PILAR QUINTERO CASELLES** por su apoyo incondicional y gran ejemplo de mujer trabajadora y luchadora, gracias a ti estoy logrando mis objetivos y metas propuestas.

A mi prometida **MISCHELLE GALITH DELGADO QUICENO** por su amor y dedicación en esta etapa de mi vida.

A mis hermanos **ANA CRISTINA PALMERA QUINTERO YRAFAEL ANDRES PALMERA QUINTERO** por apoyarme incondicionalmente y compartir conmigo cada momento de mi vida, pero sobre todo por ser ese motor que hace que logre mis objetivos convirtiéndome en un luchador incansable.

Y a mis compañeros de estudios quienes han compartido conmigo en este camino y hoy ven esta meta cumplida. ¡Vamos por la siguiente!

LUIS MANUEL PALMERA QUINTERO

DEDICATORIA

A Dios

Por haberme permitido culminar esta gran etapa de mi vida y quien me dio fortaleza cada vez que pensaba que no podía más, gracias Dios por tu infinita bondad y misericordia, por no dejarme desfallecer y ser la luz al final del camino y por permitirme hoy estar aquí.

A mi madre Rosa Leda Villero Orozco

Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, por el valor mostrado para salir adelante, pero más que nada por su amor y dedicación.

A mis familiares

Por su apoyo incansable, por ser parte de esta etapa y ser un ejemplo a seguir, por su perseverancia.

A mis amigos

Que nos apoyamos mutuamente para culminar esta etapa de nuestra vida, por enseñarme el valor de la amistad.

EDGAR MUÑOZ VILLERO

AGRADECIMIENTOS

Agradecemos a **“DIOS”** ser supremo y creador de todas las cosas, por darnos la inteligencia, sabiduría y constancia para lograr cada meta propuesta.

A la Ingeniera **ANA MELISSA RODRIGUEZ CHINCHILLA** por el tiempo, orientación y aportes que nos brindó para consolidar este nuevo logro.

Y a todas aquellas personas que lograron orientarnos y motivaron para el desarrollo de ésta especialización.

Índice

Lista de Figuras

Lista de Tablas

Introducción

En la actualidad, la información es uno de los activos más valiosos de cualquier empresa debido a su valor, la información toma importancia solo cuando se utiliza de una forma adecuada, y además está disponible en el momento indicado, dichos activos se deben utilizar de manera íntegra, oportuna, responsable y segura, deben tener una adecuada gestión de sus recursos y activos de información, ya que tiene como objetivo asegurar y dar el mejor tratamiento al uso de la información. La cantidad y complejidad de la información siguen teniendo un aumento considerable y se enfrentan cada día a riesgos y amenazas; debido a esto, las empresas necesitan proteger y reforzar su activo más valioso: “la información”.

Los riesgos y las vulnerabilidades dentro de la empresa pueden representar problemas graves y difíciles de anticipar, por esta razón es importante que la información se convierta en una herramienta estratégica para combatir los posibles ataques. Por ese motivo es necesario planificar un Sistema de Gestión de la Seguridad de la Información basado en la Norma ISO 27001:2013 y controles ISO 27002:2013, que permita prevenir y tratar cualquier tipo de amenaza que pueda poner en riesgo la continuidad de la empresa.

El presente trabajo se desarrolló con la finalidad de planear los procesos, responsabilidades y tareas que se establecerán en el Sistema de Gestión de la Seguridad de la Información en la empresa FQ Tecnologías en la ciudad de Valledupar, esta propuesta contempla un grupo de controles requeridos a partir de los hallazgos encontrados en las auditorías realizadas con anterioridad.

Capítulo 1: Planteamiento Del Problema

FQ Tecnologías cuenta con una serie de elementos tecnológicos que dan soporte al procesamiento de información (hardware y software); a través de los años los elementos tecnológicos de la empresa van cambiando con el fin de mejorar la infraestructura tecnológica sin tener en cuenta la necesidad de acompañar este proceso de cambio de una adecuada gestión de la seguridad de la información. De otro modo Santiago & Sánchez, (2017) consideran "la información como la materia prima en la operación de las organizaciones en un mundo globalizado como este, en el que los consumidores se hacen más exigentes". De otro modo Solarte (2015) y Benavides (2015) explicaron la importancia de los sistemas de información, y los datos contenidos en ellos son los activos más valiosos para las organizaciones empresariales y se hace necesario brindarles una protección adecuada. No obstante Santiago & Sánchez, (2017) por su parte explican que "la tecnología es la herramienta clave para reducir los tiempos de respuesta en la atención al consumidor, permitiendo expandir las fronteras del mercado y hacerse cada vez más competitivo". Como resultado de la investigación de Daniel Felipe González, (2014) "los gerentes o propietarios cuando elaboran planes estratégicos y crean objetivos organizacionales normalmente no están conscientes que el mundo electrónico está lleno de riesgos y amenazas que se puedan presentar en cualquier momento"; como resultado de la investigación anteriormente citada arrojan como resultado:

- 81% de las empresas nunca ha implementado una herramienta para gestión de riesgos.
- 40% No revisa el marco normativo de seguridad de la información implementado en la empresa.

- 47% nunca hizo ningún test de seguridad de las redes (Ethical Hacking, Análisis de Vulnerabilidades y/o Pruebas de Penetración en su empresa).
- 47% no cuenta con un Plan de Continuidad del negocio que le permita seguir con las operaciones en caso de un evento no deseado.

La globalización de los Sistemas de Gestión de Seguridad de la información a nivel mundial, hace necesario que los países y/o empresas diseñen planes estratégicos donde aplican elementos claves para el mejoramiento continuo de los procesos de seguridad, la calidad, la prevención de perdida de la información, tal como lo expresa el Primer Ministro de Francia Manuel Valls (2017), “Francia está plenamente comprometida en la transición digital, donde se consolida el Sistema de Gestión de Seguridad de la información expuesto en un proyecto de Republica Digital, donde pueda contrarrestar la perdida de información en las empresas”.

A nivel nacional se observa claramente, el apoyo de comenzar proyectos para Diseñar Un Sistema de Seguridad de la Información para una entidad financiera de segundo piso, bajo los lineamientos de la norma ISO/IEC 27001:2013; ya que es un herramienta de gran ayuda que permite identificar los diferentes aspectos que se deben tener en cuenta, logrando obtener una serie de diagnósticos que permitieron establecer el nivel de madurez de la entidad frente a la gestión de la seguridad de la información. (Guzman Silva C. , 2015) A nivel local en el 2012, es presentado en la Universidad Francisco de Paula Santander Ocaña un proyecto mediante el cual un Sistema de Gestión de Seguridad de la Información para el área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar; minimizara considerablemente el riesgo de su productividad y esta se vea afectada debido a la ocurrencia de un evento que comprometa la confidencialidad,

disponibilidad e integridad de la información o de alguno de los sistemas informáticos. (Casadiegos Santana, Quintero Jiménez , & Toro Rueda, 2012)

FQ tecnologías, es una empresa que está comprometida con el crecimiento de la industria tecnológica, principalmente en la región del caribe colombiano, esta tiene como obligación cumplir con las normativas vigentes, con respecto a garantizar la seguridad, protección y privacidad de la información financiera y personal de las diferentes empresas que se encuentra en su base de datos. Independientemente de la manera como la información se reciba, se comparta o almacene, se debe tener una adecuada protección, sin embargo, la seguridad informática establecida por la empresa en este momento es limitada e insuficiente. Cabe resaltar que la seguridad total es inalcanzable, lo que se pretende es garantizar que los riesgos que afronta la empresa en términos de seguridad de la información sean conocidos por la alta gerencia a fin de determinar si serán, asumidos, gestionados o minimizados. Esta preocupación debe ser adecuadamente atendida para así mantener la operatividad y rentabilidad de la empresa.

1.1 Formulación del problema

¿MEDIANTE LA PLANIFICACION DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION BASADO EN LA NTC ISO 27001:2013, ES POSIBLE DISEÑAR UN INSTRUMENTO QUE PERMITA GESTIONAR LOS RIESGOS ASOCIADOS AL PROCESAMIENTO Y ALMACENAMIENTO DE LA INFORMACIÓN PARA LA EMPRESA FQ TECNOLOGÍAS S.A.S?

1.2 Objetivos (General Y Específicos)

General

- Planear el Sistema de Gestión de Seguridad de la Información para la empresa FQ Tecnologías S.A.S, basado en la norma NTC ISO 27001:2013.

Específicos

- Diagnosticar el estado actual de la seguridad de la información de la empresa FQ Tecnologías S.A.S, teniendo en cuenta los dominios aplicables de la norma NTC ISO 27001:2013.
- Identificar y analizar los riesgos de seguridad de la información presentes en la empresa.
- Documentar la planeación del SGSI para la empresa FQ Tecnologías S.A.S

1.3 Justificación

La planificación de un Sistema de Gestión de Seguridad de la Información basado en un modelo de buenas prácticas de seguridad conocido a nivel mundial, como lo es la NTC ISO 27001, proveerá las condiciones de gobernabilidad, oportunidad y viabilidad necesarias para que la seguridad de la información apoye y extienda los objetivos Misionales y Estratégicos de la empresa, mediante la protección y confidencialidad de información que es fundamental para

garantizar los debidos procesos en la oficina de Extensión y Proyección Tecnológica, y con ello asegurar el cumplimiento de la Misión y Visión.

Teniendo en cuenta el creciente aumento de amenazas informáticas que buscan sustraer de las empresas su información, es acertado que FQ TECNOLOGIAS cuente con las tecnologías a la vanguardia de la seguridad de la información, es necesario contar con procesos estructurados y personal especializado que maneje incidentes de seguridad de información y restablezcan los temas en el menor tiempo posible. Guzman, (2015) mencionó: “La planeación y posterior operación de un SGSI no es obligatoria para la empresa, poder contar con un grupo de Políticas aprobadas por la Gerencia se reconocería como un paso principal para brindar dirección y alineamiento para los diferentes procesos Misionales o de Apoyo”.

Con una adecuada Gestión de la seguridad de la información la empresa FQ tecnología, contara con una serie de herramientas que les permitirán a sus directivos tomar decisiones adecuadas y oportunas con relación a las falencias presentadas en el sistema que administra los procesos operativos. De igual forma le facilitara mejorar la administración de la información de los clientes a través de la inclusión de procesos, procedimientos y políticas que promuevan una cultura llena de buenas prácticas de seguridad de la información al interior de la empresa. Que a su vez generara mayor rentabilidad dentro de un marco de mejora continua.

1.4 Delimitaciones

Delimitación Operativa: El desarrollo del proyecto desde el punto de vista operativo se soporta en los procesos principales de la empresa FQ Tecnologías.

Delimitación Conceptual: Los conceptos que se van a manejar en este proyecto se relacionan con los Sistemas de Gestión de Seguridad de la Información, Políticas de Seguridad de la Información, Gestión de Riesgos, Gobernabilidad de TI.

Delimitación Geográfica: La ubicación de la empresa donde se llevará a cabo el desarrollo de esta norma y donde se hará el respectivo análisis y la recolección de datos pertinentes es en la Carrera 3 # 13b-49 de la ciudad de Valledupar, Cesar.

Delimitación Temporal: El periodo de realización del estudio será de 4 semanas a partir de la aprobación del proyecto.

Capítulo 2: Marco Referencial

2.1 Marco histórico

La historia de la Seguridad de la Información, desde la antigüedad, los mensajes cifrados han jugado un papel muy importante en el mundo tecnológico, ya que surge la necesidad de transmitir y almacenar la información de forma confidencial y encriptada, en los últimos años la preocupación de las empresas por la seguridad de la información ya que esta representa mucho valor, este debe clasificarse como un activo esencial para la empresa y velar por asegurar su protección. Los avances en la tecnología, aparte de las múltiples ventajas en el procesamiento y análisis de información, ocasiona un gran riesgo al mundo de la informática; debido a que la información en formato digital o en la nube, es más fácil de transportar, por lo que las posibilidades de alterarlas o tomarlas sin autorización no son despreciables. Con relacion a lo anterior Castilla, Echavez, Rodriguez y Sandoval (2014), explican que, “la evidencia con la que cuenta una empresa para poder enfrentarse a entidades de control en cuanto a demandas y procesos judiciales se refiere es a la información”.

La seguridad de la información toma relevancia en el año 1980 en donde se fundamentan las bases de la seguridad de la información, en este año, James P. Anderson escribe un documento titulado ‘Computer Security Threat Monitoring and Surveillance’. Lo mas interesante de este documento es que James Anderson da una definición de los principales agentes de las amenazas informáticas. (Castilla, et al. 2014, p.14)

2.2 Marco teórico

Con el pasar de los años la seguridad de información ha tomado una mayor importancia, lo que trajo consigo que un grupo de especialistas a nivel mundial en temas relacionados a seguridad, riesgos y temas afines, desarrollen diversos marcos de trabajo, metodologías, estándares, buenas prácticas, distintos modelos para diseñar un SGSI, leyes, normativas, entre otros, con la finalidad de brindar a las empresas la oportunidad de adoptarlas y proteger adecuadamente la información de sus clientes.

ISO/IEC 27001: es una norma internacional referente para la gestión de seguridad de la información que cubre todo tipo de organización incluidas las gubernamentales y entidades sin animo de lucro, y especifica los requisitos para establecer, implementar, supervisar y mejorar un sistema de seguridad de la información (SGSI). (TUV SUD, 2013)

NTC ISO 31000:2011 Gestión del Riesgo: se hace necesaria para controlar y manejar las amenazas que se presentan a nivel organizacional y tecnológico, con los recursos disponibles, a fin de que no se materialicen estos riesgos y afecten los productos y/o servicios que ofrece la empresa.Aunque todas las organizaciones gestionan el riesgo en algún grado, esta norma establece un número de principios que es necesario satisfacer para hacer que la gestión del riesgo sea eficaz. (Cárdenas Herrera & Higuera Soto, 2016)

Sistemas de Gestión de la Seguridad de la Información: provee un modelo para establecer, implementar, monitorear, revisar, mantener y mejorar la protección de los activos informáticos

para lograr los objetivos organizacionales basados en una gestión del riesgo y en los niveles aceptables de riesgos diseñados efectivamente para tratarlos y gestionarlos, analizando los requerimientos para la protección de los activos informáticos y aplicando los controles apropiados para asegurar que la protección de estos activos contribuyen a la implementación exitosa del mismo. (Doria Corcho, 2015)

Amenazas a la Seguridad de la Información: la infraestructura de TI de una organización está compuesta por activos. Un Recurso Informático, se define como todo aquello que puede generar valor para la empresa y que estas sientan la necesidad de proteger. Un activo esta representado por los objetos físicos (hardware, routers, switches, hubs, firewalls, antenas, computadoras), objetos abstractos (software, sistemas de información, bases de datos, sistemas operativos) e incluso el personal de trabajo y localidades físicas. (Doria Corcho, 2015)

Ciclo PHVA: para monitorear y adoptar el proceso de planeación de un sistema de gestión se usa el modelo P.H.V.A (planear, hacer, verificar y actuar), el cual permite planear, tomar acciones, verificar los resultados y actuar sobre los resultados esperados. (Rodríguez Correa, 2017)

El ciclo PHVA consiste básicamente en:

- **Planear:** definen las metas y los métodos para alcanzarla.
- **Hacer:** despues de haber realizado un proceso de formación se ejecutan y recogen todos los datos.

- **Verificar:** se evalúan los resultados e identifican los problemas no resueltos.
- **Actuar:** se toman las medidas correctivas necesarias para el cumplimiento de las metas.

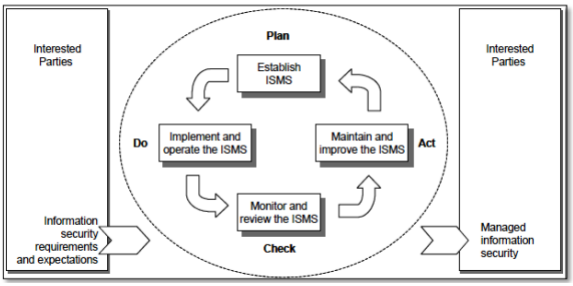


Ilustración 1. Modelo PHVA aplicado a los procesos de un SGSI

Fuente: *ISO/IEC International Standard ISO/IEC 27000: Information Tecnology*

Política de Seguridad: son establecidas por la Dirección de la empresa y tiene en consideración que:

- Ha de adecuarse a la estrategia de la empresa.
- Ha de reflejar los objetivos de seguridad de la información y un marco para ella.
- Ha de reflejar un compromiso y deber por parte de la audiencia de la politica.
- Ha de estar disponible y constatemente comunicada a las personas que afecte.

La políticas de Seguridad de la empresa reconoce como activo estratégico y fundamental la información, por lo que debe ser utilizada y mantenida con las medidas de protección que, como activo de gran mportancia, merece. Es necesario tener en cuenta que la información vital en la consecución de los objetivos de la misma. (Lievano Cos, 2016)

Gestión del Riesgo: es un proceso cuya función principal es mantener un ambiente seguro. Consiste en identificar los factores que podrian dañar o revelar datos, y crear medidas que implementen una solución para mitigar o reducir el riesgo. Como profesionales en el campo de la seguridad de la información, se deben conocer ciertos conceptos que van ligados al riesgo como lo son las amenazas, vulnerabilidades e impacto. (Doria Corcho, 2015)

- **Vulnerabilidad:** es una falla o debilidad en los procedimientos, diseño, implementación o controles internos en un sistema de seguridad.

- **Amenaza:** es el potencial que un intruso o evento explote una vulnerabilidad especifica. Es cualquier probabilidad que pueda ocasionar un resultado indeseable para la organización o para un activo en especifico.

- **Impacto:** se refiere a la cantidad de daño que pueda causar la amenza para que explote una vulnerabilidad.

2.3 Marco contextual

El desarrollo de la investigación se llevara a cabo en la empresa FQ Tecnologías de la ciudad de Valledupar, Cesar, donde se planificara un Sistema de Gestión de Seguridad de la Información basado en las NTC/ISO 27001:20013. FQ Tecnologías es una empresa solida que ofrece servicios garantizados, logrando competitividad por medio de la Tecnología de la información.

2.4 Marco conceptual

Seguridad de la información: La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo en la empresa y maximizar el retorno de las inversiones y las oportunidades comerciales. (Gerrero Melo & Suarez Castrellon, 2012)

Identificación de activos de información: de acuerdo con la norma ISO/IEC 27001, "activo de información" se define como cualquier elemento que tenga valor para la organización y, en consecuencia, deba ser protegido.

Riesgos informáticos: se define como "la probabilidad de que una amenaza en particular expone a una vulnerabilidad que podría afectar a la organización", o como "la posibilidad de que algo pueda dañar, destruir o revelar datos u otros recursos". Rodríguez (2017), explica, que, para poder tener una mayor definición del significado de riesgo en el contexto de la seguridad de la información; se divide en 4:

- **Evento:** en el contexto de la evaluación de riesgos es siempre un evento futuro y tiene influencia directa o indirecta sobre el resultado.

- **Activo:** un activo es algo valioso para la empresa y en el contexto de seguridad informática están constituidos por el software, el hardware, las aplicaciones, las bases de datos, las redes, copias de seguridad e incluso los empleados.

- **Resultado:** en el contexto de la seguridad informática siempre será una circunstancia no deseada como una pérdida o pérdida potencial. Esta pérdida tiene un efecto directo en la mayor parte de los activos de las empresas.

- **Probabilidad:** posibilidad o frecuencia de que un evento ocurra sobre un activo.

Tratamiento del riesgo: selección e implementación de las opciones apropiadas para ocuparse del riesgo.

Valoración del riesgo: proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.

Vulnerabilidad del riesgo: debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

Control: es un proceso por el cual la administración verifica si lo que ocurre concuerda con lo que supuestamente debe ocurrir. Permite que se realicen los ajustes o correcciones necesarias en caso se detectan eventos que escapan a la naturaleza del proceso. (Casadiegos Santana, Quintero Jiménez , & Toro Rueda, 2012)

Direccionamiento Estratégico: es una disciplina que integra varias estrategias, que incorporan diversas tácticas. El conocimiento, fundamentado en información de la realidad y en la reflexión sobre las circunstancias presentes y previsibles.

Política de seguridad de la información: es un conjunto de normas o prácticas para regular la forma en que se usa, protege y distribuye la información y los sistemas de información con el fin mitigar el riesgo de pérdida, deterioro o acceso no autoriza a la misma. (Rodríguez Correa, 2017)

2.5 Marco legal

- **Manual de Normas y Políticas de Seguridad de la Información:** establece reglas y lineamientos técnicos para el uso controlado de activos de información que minimice el riesgo de pérdida de datos, accesos no autorizados, divulgación no controlada, duplicación e interrupción intencional de la información. (Oficina TIC Los Patios, 2017)

- **Manual de Políticas de Seguridad de la Información:** establecer las políticas que regulan la seguridad de la información en el departamento administrativo de la presidencia de la República DAPRE y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el DAPRE, bajo el liderazgo del Área de Tecnologías y Sistemas de Información. (SIGEPRE, 2018)

- **Resolución Número 01760 de 09 FEB 2018:** se creó el Sistema de Gestión de Seguridad de la información estableciendo los lineamientos generales de la Estrategia de Gobierno en Línea. (MINISTERIO DE EDUCACIÓN NACIONAL, 2018)

- **Resolución número 08310 de 28 Dic 2016:** por el cual se expide el Manual del Sistema de Gestión de Seguridad de la información para la policía Nacional. (MINISTERIO DE DEFENSA NACIONAL , 2016)

- **Decreto Número 2573 de 12 DIC 2014:** contiene normas para Objeto, ámbito de aplicación, definiciones, principios y fundamentos según el Ministerio de Tecnologías de la Información y las Comunicaciones. (Ministerio de Tecnologías de la información y las comunicaciones , 2014)

- **Modelo de Seguridad y Privacidad de la Información:** conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos. (MINTIC)

Capítulo 3: Diseño metodológico

3.1 Tipo de investigación

De acuerdo a las características del proyecto, se empleará el tipo de investigación descriptiva, con aportes de herramientas cuantitativas. La investigación descriptiva brinda una metodología apropiada para recolectar información básica para llevar a cabo el proyecto, ya que la misma describe de modo sistemático las características de una población, situación o área de interés.

La línea de investigación para la elaboración del proyecto, se enmarcó en el Gobierno de TI, y los conceptos utilizados se relacionaron con temas como: tecnología de la información, seguridad de la información, gestión de la seguridad, gestión de riesgos y sistema de gestión de seguridad de la información.

3.2 Población y muestra

Teniendo en cuenta el tipo de estudio escogido, se procede a establecer el conjunto de elementos a estudiar definidos de la siguiente manera:

3.2.1 Población.

En cuanto a la población objeto de estudio se tomaron en cuenta todos los funcionarios que conforma la empresa FQ Tecnologías.

3.2.2 **Muestra.** Debido a que la población es limitada, se trabajó como muestra toda la población que conforma la empresa FQ Tecnologías.

3.3 Técnicas de recolección de la información

Para el desarrollo del proyecto se realizó a través de una investigación descriptiva que es aquella que describe de modo sistemático las características de una población, situación o área de interés. En esta fase se diseñaron los instrumentos de recolección de la información, se aplicaron y se analizaron con el fin de obtener la información necesaria para el desarrollo y cumplimiento de los objetivos.

Con la aplicación de este método de investigación se obtuvo un diagnóstico situacional de la empresa FQ TECNOLOGIAS S.A.S.

3.3.1 **Fuentes Primarias.** La información primaria se obtendrá a través de entrevistas al Gerente, Contador, Auxiliar contable, Secretaria de Gerencia y del encargado del Área de Sistemas y la observación directa de las actividades que se desarrollan en la empresa FQ Tecnologías, lo cual se identificara cada uno de los procesos y los riesgos de la empresa.

3.3.2 Fuentes secundarias. Las fuentes secundarias serán obtenidas a través de libros, publicaciones, artículos, consultas en internet y textos adicionales con información afín a la investigación.

3.4 Costos del proyecto

A continuación, se describe el costo de todos los servicios, materiales, equipos, software y talento humano que son necesarios para la ejecución de este proyecto.

3.5 Materiales

Los materiales son herramientas básicas que son necesarias para los cumplimientos de los objetivos y documentación del proyecto.

Tabla 1. *Costo material*

COSTO DE MATERIALES			
MATERIALES	**CANTIDAD**	**PRECIO VALOR UNITARIO**	**VALOR TOTAL**
Lapicero	4	1.000	$ 4.000
Libreta de Apunte	1	10.000	$ 10.000
Papel (Resma)	2	11.000	$ 22.000

Disco Compacto	6	1.500	$ 9.000
TOTAL			**$ 45.000**

3.6 Equipos

En el esquema siguiente se referencian lo equipos utilizados durante la realización o desarrollo del proyecto.

Tabla 2. *Costo De Equipo*

EQUIPO UTILIZADO	CANTIDAD	VALOR EN PESOS
Computador Portátil HP	1	$ 1.500.000
Computador Portátil Lenovo	1	$ 1.500.000
Memoria USB	2	$ 50.000
TOTAL		$ **3.050.000**

3.7 Recursos humanos

Durante el proceso desarrollo del proyecto fue necesario replantear ideas, aclarar dudas, profundizar sobre el conocimiento del entorno de desarrollo.

Tabla 3. *Costo De Recursos Humanos*

ACTIVIDAD	COSTO/DÍA	HORAS	TIEMPO	TOTAL
Auditor 1:	45.000	9 horas semanal	4 semanas	$ 1.620.000
Auditor 2:	45.000	9 horas semanal	4 semanas	$ 1.620.000
TOTAL				**$ 3.240.000**

3.8 Servicios

A continuación, se describe los costos que son necesario para que el desarrollo e implementación del aplicativo.

Tabla 4. COSTO DE LOS SERVICIOS

TIPO DE SERVICIO	TIEMPO	VALOR
Servicio de Transporte	4 Semanas	$ 200.000
Servicio de Internet	4 Semanas	$ 100.000
Servicio de Impresión	N/P	$ 90.000
Servicio de diseño e impresión de Label	N/P	$ 40.000
Total		**$ 430.000**

Tabla 5. *Total*

TIPO DE SERVICIO	VALOR
Costo de Material	**$ 45.000**
Costo de Equipo	**$ 3.050.000**
Costo de Recursos Humanos	**$ 3.240.000**
Costo de los Servicio	**$ 430.000**
TOTAL	**$6.725.000**

De los resultados arrojados por cada tabla se obtiene un valor aproximado para la inversión de este proyecto de seis millones setecientos veinte cinco mil pesos ($ 6.725.000).

Capítulo 4: Presentación de resultados

Para el logro de los objetivos propuestos se implementaron una serie de actividades

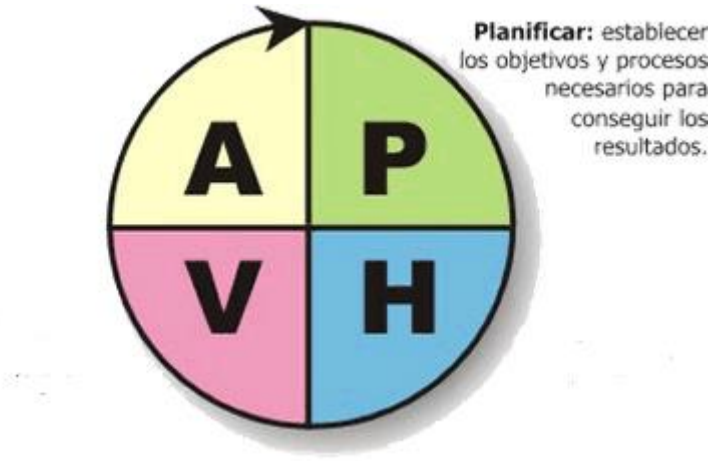
Tabla 6. *Actividades por objetivo*

OBJETIVOS	ACTIVIDADES	RESULTADOS
Diagnosticar el estado actual de la seguridad de la información de la empresa FQ Tecnologías S.A.S, teniendo en cuenta los dominios aplicables de la norma NTC ISO 27001:2013.	1. Recopilar información de la empresa: Misión, Visión, objetivos, procesos entre otros. 2. Diseñar instrumentos de recolección de datos (Lista de chequeo, Encuesta, Entrevista, Papeles de trabajo.) 3. Auditoria.	1. Modelado de Negocio de la empresa. 2. Instrumentos de recolección. 3. Informe Preliminar de auditoria.
Identificar y analizar los riesgos de seguridad de la información presentes en la empresa.	1. Investigar los elementos que estructuran un SGSI. 2. Adaptar al contexto de la empresa los	1. Elementos SGSI. 2. Nivel de Madurez (Tabla 8). 3. Niveles de Riesgo (Tabla 7).

	dominios de seguridad física y lógica. 3. Analizar los riesgos.
Documentar la planeación del SGSI para la empresa FQ Tecnologías S.A.S	1. Identificación de alcances y objetivos. 2. Crear una Política de Seguridad de la Información basada en la norma ISO 27001:2013.

Fuente: Autores del Proyecto.

Ilustración 2. Metodología PHVA



Fuente: Adaptación de los autores del proyecto

4.1 Diagnostico

Diagnosticar los elementos organizacionales de la empresa FQ Tecnologías a través de una auditoria pasiva con base a la norma ISO7iec 27001:2013.

4.1.1 Modelado del Negocio. FQ TECNOLOGIAS S.A.S fue creada el 14 de junio del 2014 por iniciativa de los Ingenieros JAIME FUENTES y JORGE YAGUNA, quienes deciden crear una compañía sólida que ofrezca servicios garantizados y contribuir al logro de la Competitividad por medio de la Tecnología de la información. En esta etapa solo tres trabajadores estaban ligados a la empresa incluidos sus cofundadores y un Ingeniero de sistema, inician sus primeros proyectos. Con este pequeño equipo enfrentan este gran reto.

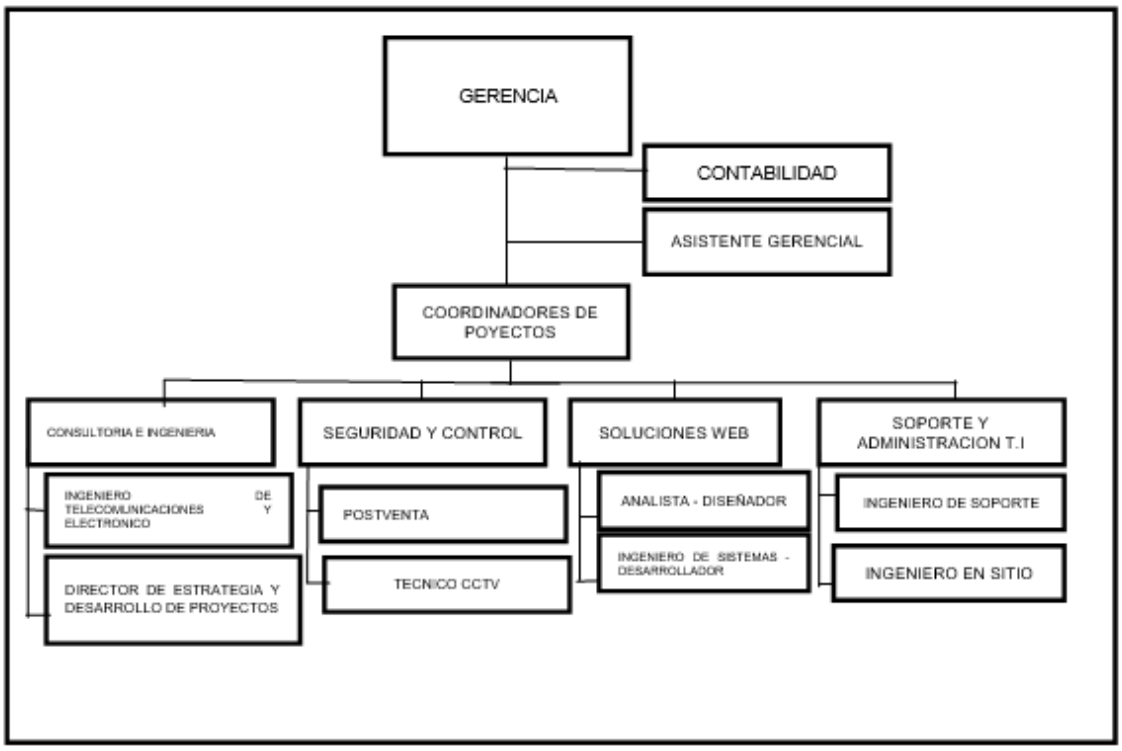
En el mes de agosto de ese mismo año fue constituida legalmente como **FQ TECNOLOGIAS S.A.S,** al poco tiempo se convirtieron en partner autorizados por Google para la venta, configuración y soporte técnico de G Suite en Colombia, este fue un logro muy importante ya que era uno los principales objetivos a cumplir planteado inicialmente.

Luego en 2015 empezaron a trabajar en proyectos de gran magnitud a nivel regional esto, obligo a la empresa a contratar más personal capacitado para las tareas y poder cumplir con todos los objetivos propuestos en cada uno de sus trabajos.

Después de varios meses de preparación en julio de 2017 se le otorgo marca Colombia TI Insignia conferida por MinTIC como certificación de ser exportadores de la industria TI de alta calidad en Colombia. Con todos estos logros no es extraño que se hayan convertido en la primera empresa exportadora de servicios de la región haciendo proyectos para empresas en el extranjero.

FQ tecnología ha logrado un gran éxito en el poco tiempo que ha pasado desde su creación y se proyecta como una de las empresas líder en prestación de servicios de la industria TI.

Ilustración 3. Organigrama de la Empresa FQ Tecnologías



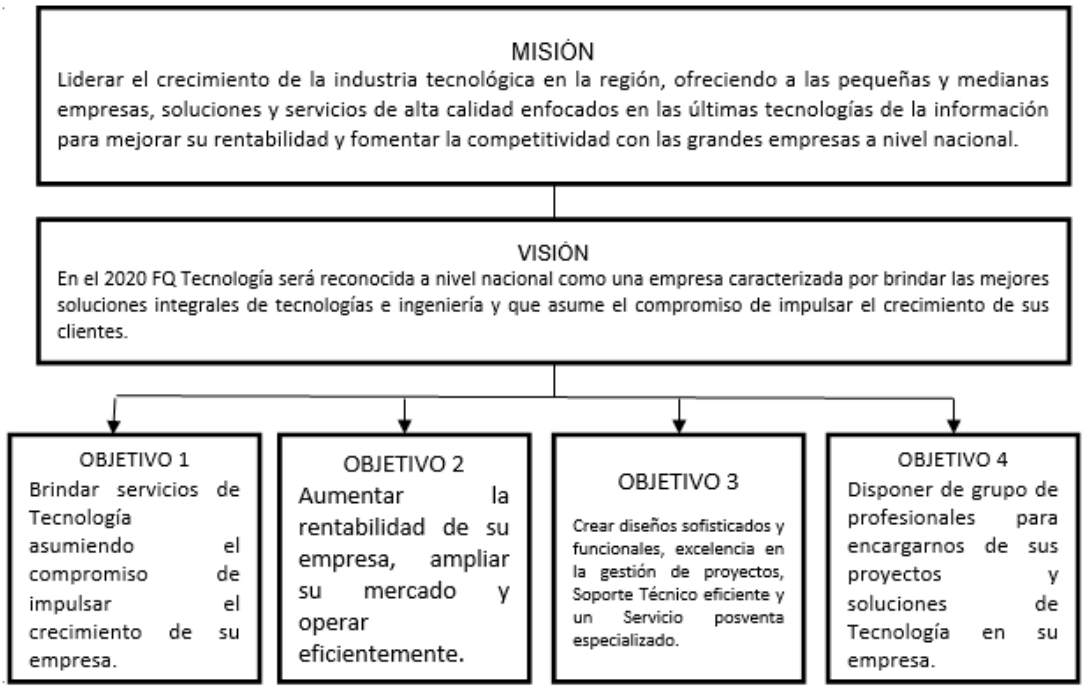
Fuente: Autores del Proyecto

Modelo de Objetivos. La empresa FQ Tecnologías, vincula directamente su objetivo general con la misión y visión de la empresa. (Ilustración 4.)

Objetivo General

Consolidación empresarial en la ciudad de Valledupar en el sector tecnológico.

lustración 4. Misión, Visión y Objetivos de la empresa FQ Tecnologías



Fuente: Autores del Proyecto.

Ilustración 5. Misión y Visión Propuestas

MISIÓN

Liderar el crecimiento de la industria tecnológica en la región, ofreciendo a las pequeñas y medianas empresas, soluciones y servicios de alta calidad para mejorar su rentabilidad y fomentar la competitividad haciendo uso de las herramientas de TI para la consolidación de la empresa.

VISION

En el 2020 FQ Tecnología será reconocida a nivel nacional como una empresa caracterizada por brindar las mejores soluciones integrales de tecnologías e ingeniería. Trabajando con políticas de calidad y atención al cliente que garanticen la preferencia y lealtad de nuestros productos, asegurando el crecimiento y consolidación de nuestra empresa.

Fuente: Autores del proyecto.

4.1.2 Valores corporativos FQ TECNOLOGIAS

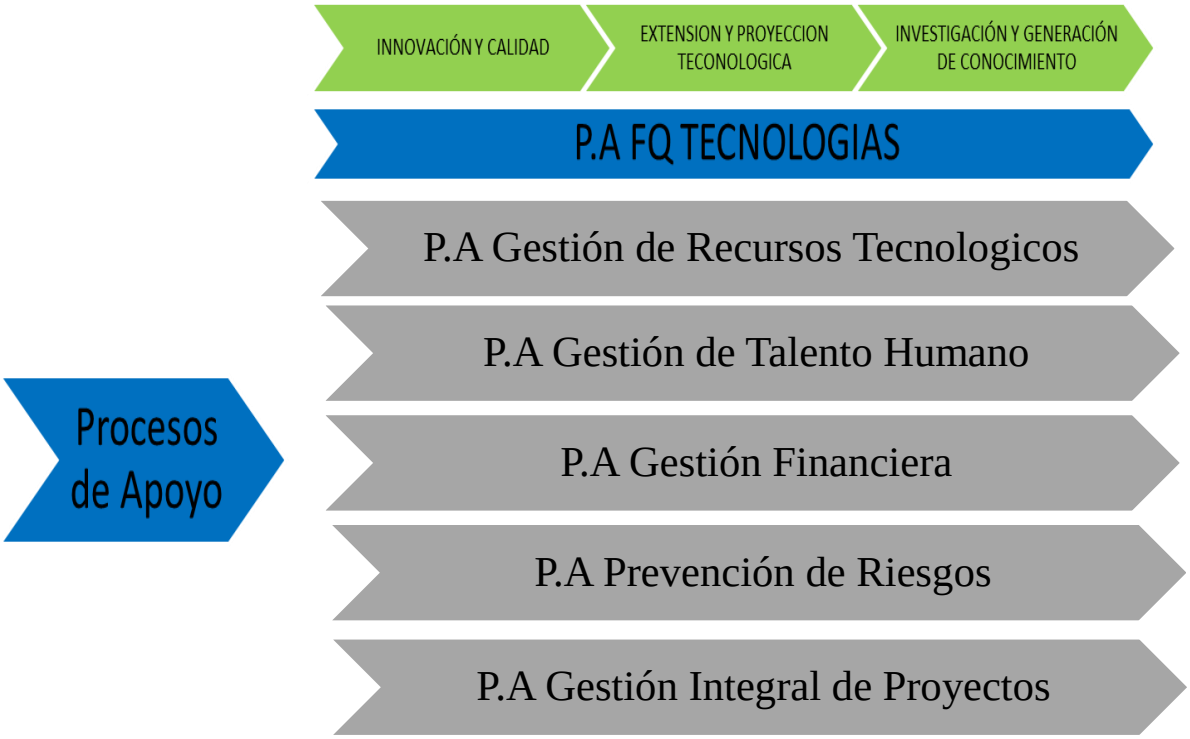
- **Capacidad para trabajar en equipo:** los empleados sobre salen por colaborar al máximo para el beneficio de la empresa.
- **Compromiso moral:** los directivos se caracterizan por su fuerte grado de implicación y compromiso en la empresa.
- **Sentido social:** la empresa es consciente de su impacto en la sociedad, sobre todo en innovación tecnológicas.
- **Responsabilidad coherente:** la empresa actúa hacia objetivos establecidos bajo una dirección única.
- **Empoderamiento:** los directivos de la empresa incentivan a sus trabajadores a dar lo mejor de sí. Por ello, son receptivos a las sugerencias de mejora de los procesos.
- **Liderazgo:** este valor corporativo es especialmente importante ya que sin capacidad de liderazgo no hay posibilidad de supervivencia en entornos empresariales hostiles y competitivos.
- **Eficiencia:** dada la escasez de recursos de la que dispone la empresa, han de ser eficientes en la utilización de recursos productivos tanto humanos, físicos, financieros y técnicos.
- **Capacidad de innovación:** la empresa hace frente a nuevos retos mediante la utilización de las herramientas de TI para mayor productividad y seguridad de la información.
- **Flexibilidad:** el alto grado de flexibilidad lleva a rápidos procesos de adaptación de la misma a entornos cambiantes, así como para poder hacer frente a nuevas necesidades de mercado.

- **Disposición para aceptar retos:** Nacido del propio espíritu emprendedor de los fundadores que desarrollan su actividad profesional, aceptando dichos retos es una condición ex ante para lograr, ex post, un proceso de creación de empleo y riqueza con su impacto correspondiente en el bienestar económico y social de los stakeholders afectados por su actividad.
- **Honestidad:** ejercer con integridad y transparencia todos nuestros actos.
- **Puntualidad:** establecer una cultura de exactitud y responsabilidad en todos nuestros compromisos.
- **Respeto:** fomentar una actitud de obediencia, en todas las relaciones personales y en todos los niveles de autoridad.
- **Responsabilidad:** ser puntual y eficaz con los compromisos adquiridos.
- **Servicio:** dar la mejor asistencia de apoyo a los demás.

4.1.3 Diagrama de Procesos

Para realizar el diagrama de procesos se consultó la documentación presentada por la empresa FQ Tecnologías en el cual no se encuentran definido los procesos misionales de la empresa, por lo tanto, se proponen tres procesos de acuerdo con su objetivo principal que es impulsar soluciones tecnológicas e ingeniería.

Ilustración 6. Cadena de valor de la empresa FQ Tecnologías.

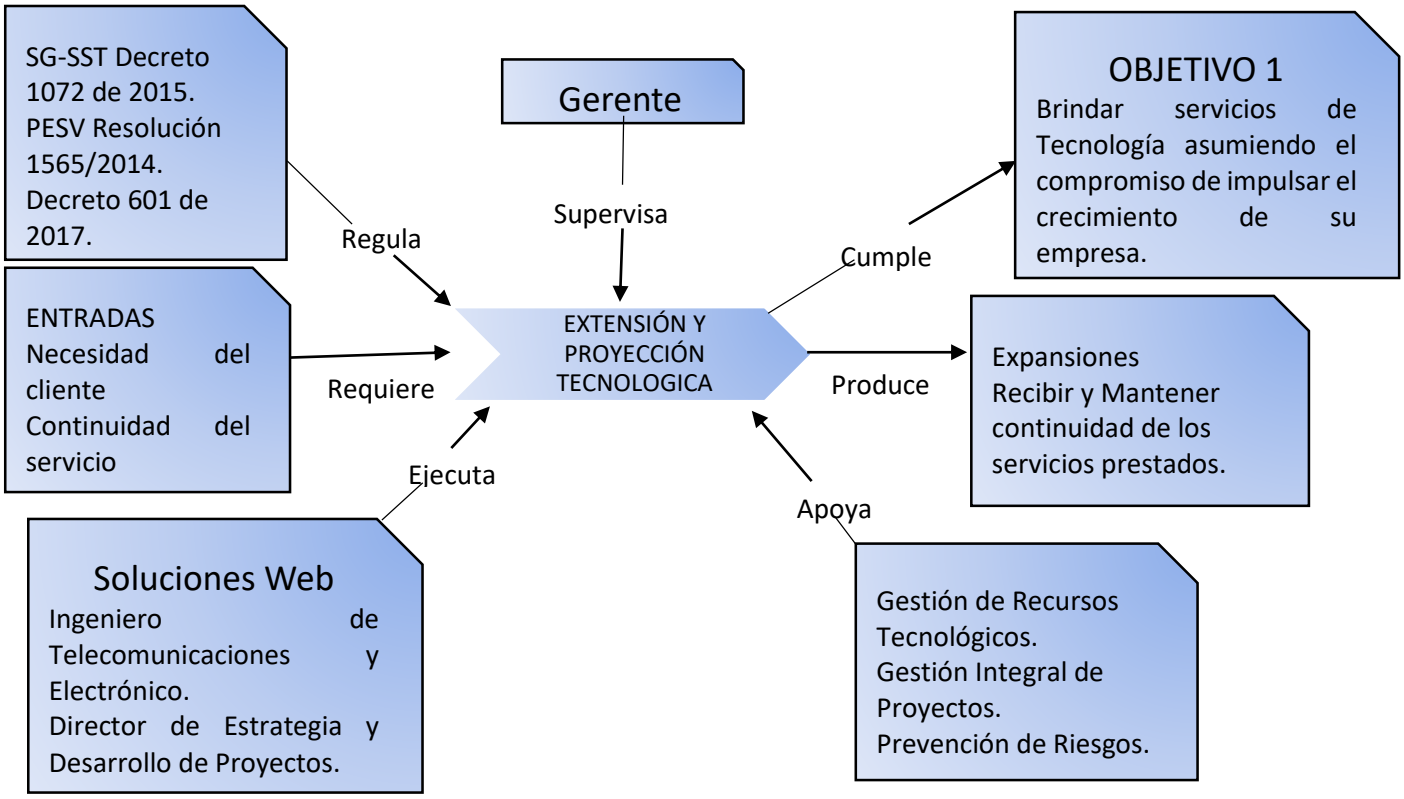


Fuente: Autores del proyecto.

PF Extensión y proyección tecnológica.

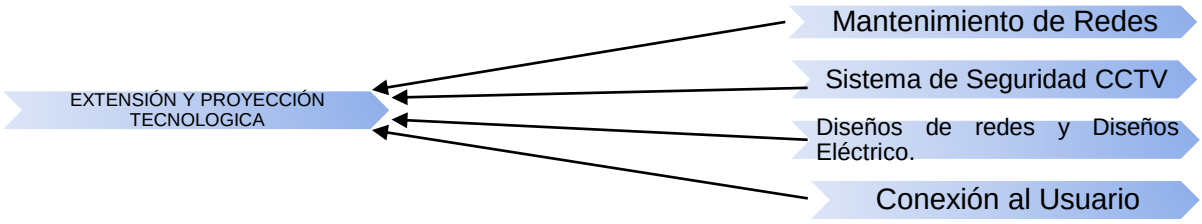
El proceso principal de Extensión y proyección Tecnológica tiene como objetivo brindar servicios de tecnología y mantener continuidad en los servicios prestados. (Su descripción puede verse en la ilustración 7).

Ilustración 7. EXTENSIÓN Y PROYECCIÓN TECNOLOGICA FQ TECNOLOGIAS



Fuente: Autores del proyecto

Ilustración 8. SUBPROCESOS EXTENSIÓN Y PROYECCIÓN TECNOLOGICA FQ TECNOLOGIAS

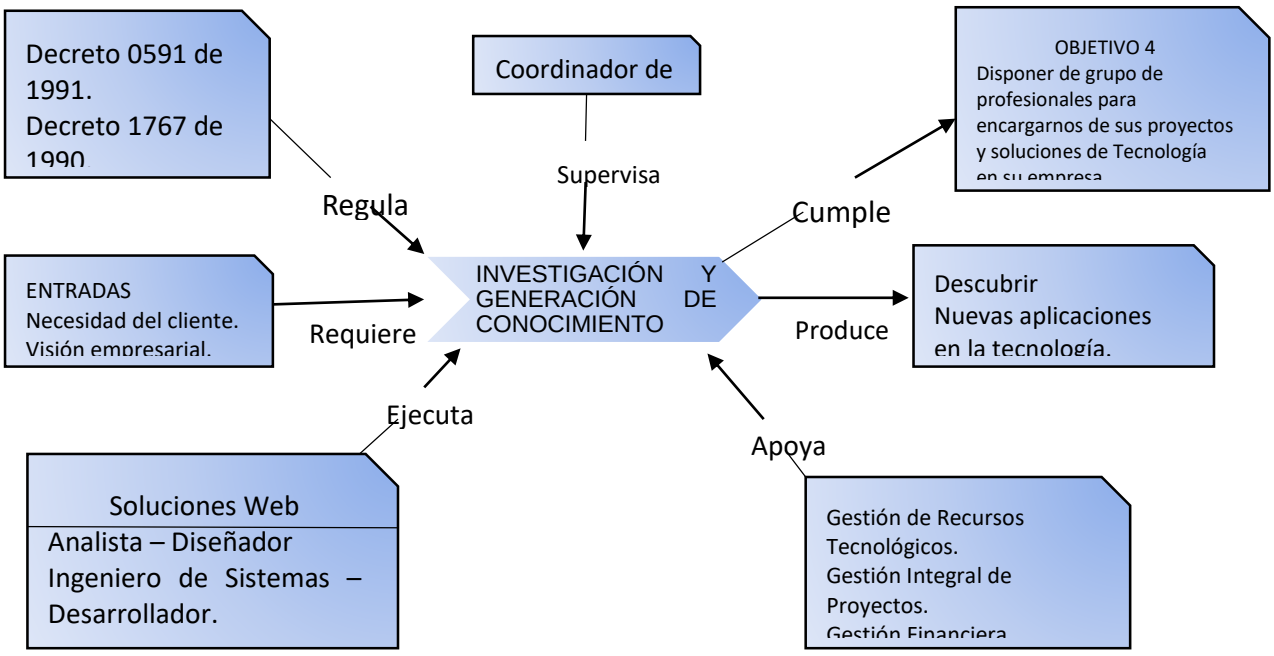


Fuente: Autores del proyecto.

PF Investigación y Generación de Conocimiento.

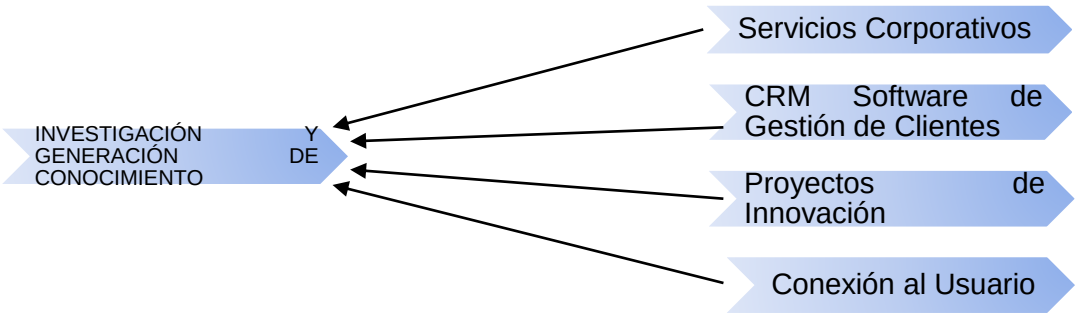
El proceso principal de Investigación y Generación de Conocimiento tiene como objetivo Disponer de grupo de profesionales para descubrir nuevas aplicaciones de TI. (Su descripción puede verse en la ilustración 9).

Ilustración 9. INVESTIGACIÓN Y GENERACIÓN DE CONOCIMIENTO FQ TECNOLOGIAS



Fuente: Autores del proyecto.

Ilustración 10. SUBPROCESOS INVESTIGACIÓN Y GENERACIÓN DE CONOCIMIENTO

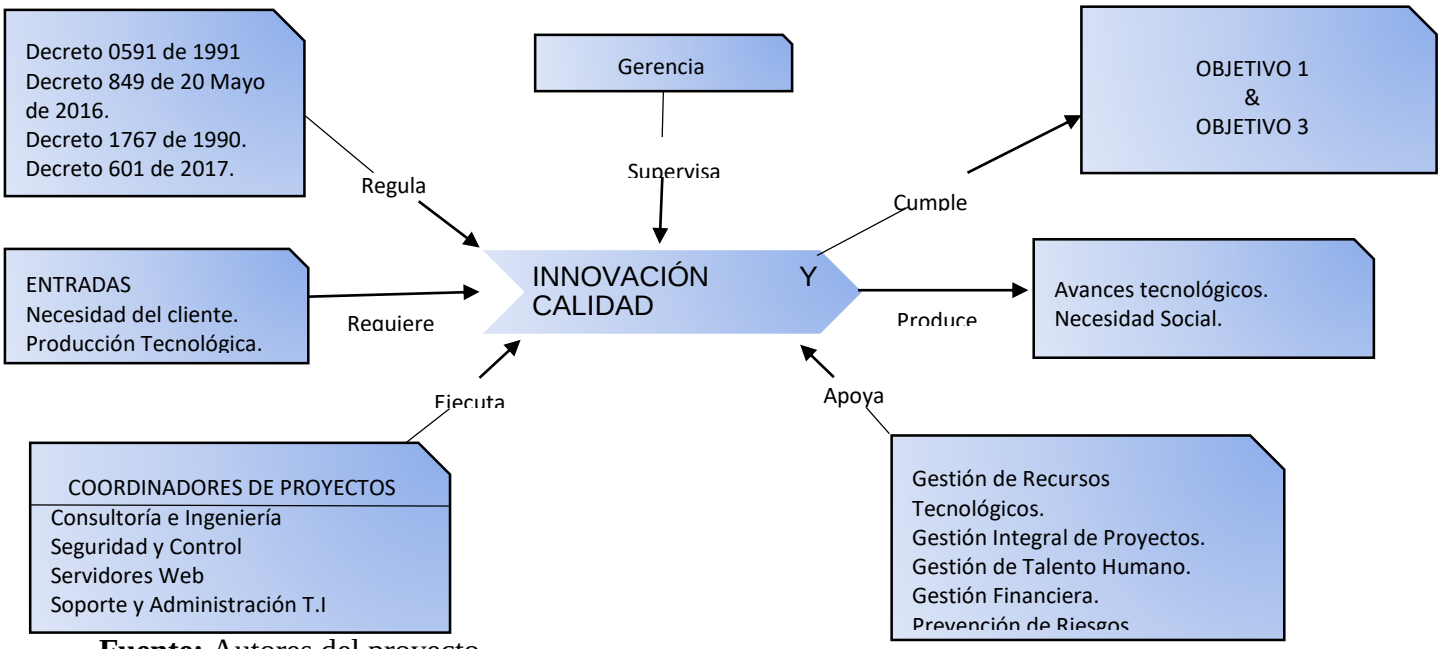


Fuente: Autores del proyecto.

PF Extensión y proyección tecnológica.

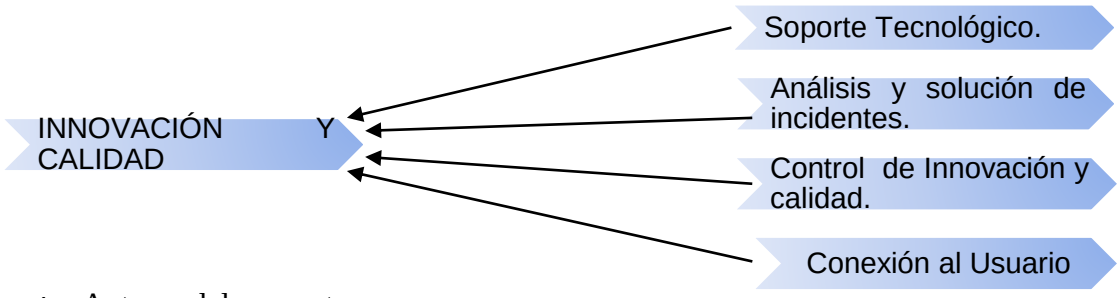
El proceso fundamental de Innovación y Calidad tiene como objetivo brindar avances tecnológicos para la ayuda de la sociedad y empresas. (Su descripción puede verse en la ilustración 11).

Ilustración 11. INNOVACIÓN Y CALIDAD FQ TECNOLOGIAS



Fuente: Autores del proyecto.

Ilustración 12. SUBPROCESOS INNOVACIÓN Y CALIDAD FQ TECNOLOGIAS



Fuente: Autores del proyecto.

4.1.4 Tecnologías de la información y las comunicaciones en FQ TECNOLOGÍAS

4.1.4.1 Sistemas de información.

FQ Tecnologías, cuenta con un sistema de información para el proceso de contabilidad creado por la misma empresa. Este software contiene informe de impuesto, informe contable, registro de movimientos, tu dinero del día, seguimiento de cobranza, cuentas por pagar, clientes, proovedores.

4.1.4.2 Infraestructura tecnológica

La empresa cuenta con una topología de red es de tipo infraestructura, tiene un elemento de coordinación: un punto de acceso o estación base. Para interconectar muchos puntos de acceso y computadores inalámbricos, todos deben configurarse con el mismo SSID. No se cuenta con un servidor en la empresa.

Ilustración 13. Topología de Infraestructura

En la ilustración se observa la Topología de Red que utiliza la empresa FQ Tecnologías que llega a través de la Línea telefónica y que este a su vez se conecta en un punto de red de un Switch/Router.

Para el funcionamiento del área administrativa la empresa cuenta con un numero de 11 computadoras portátiles de los cuales 9 son de la marca HACER de referencias E5-475 y 2 de la marca LENOVO de referencia YOGA 520-14ikb, interconectados por una Red WLAN.

4.2 Niveles de Riesgos FQ Tecnologías

Tabla 7. *Niveles de Riesgo*

NIVELES DE RIESGOS FQ TECNOLOGIAS

Actividades/ Tareas	Actividad		Peligro Clasificación	Evaluación del Riesgo		Valoración del riesgo	
	Rutinaria	No Rutinaria		Valor Probabilidad	Valor Severidad	Nivel del Riesgo	Significado
Oficios Varios	X		Biomecánicos-postura	2	2	4	Aceptable con control especifico
			Químicos-Líquidos	2	2	4	Aceptable con control especifico
			Condiciones de Seguridad-Incendio	1	2	2	Aceptable
			Biológico-Fluidos o excremento	3	2	6	Aceptable con control

						específico
Trabajos en Altura	**X**	**Condiciones de seguridad**	**3**	**4**	**6**	**Aceptable con control específico**
		Fenómenos naturales	**3**	**3**	**6**	**Aceptable con control específico**
		Biomecánicos-posturas	**2**	**3**	**2**	**Aceptable**
		Psicosocial-condiciones de la tarea	**3**	**2**	**6**	**Aceptable con control específico**
Revisión Sistemas Eléctricos	**X**	**Físico-iluminación**	**3**	**3**	**6**	**Aceptable con control**

						especific o
		Condicione s de seguridad	**3**	**3**	**3**	**Aceptabl e con control especific o**
		Fenómenos naturales	**1**	**2**	**2**	**Aceptabl e**
		Biomecánic os-posturas	**2**	**4**	**6**	**Aceptabl e con control especific o**
Actividades Administrati vas	**X**	**Físico-iluminación**	**4**	**1**	**4**	**Aceptabl e con control especific o**
		Psicosocial-condiciones de la tarea	**3**	**2**	**6**	**Aceptabl e con control**

						específico
		Biomecánicos-postura	**2**	**2**	**4**	**Aceptable con control específico**
		Condiciones de seguridad-cableado	**3**	**1**	**3**	**Aceptable**
Supervisión	**X**	**Condiciones de seguridad**	**2**	**3**	**6**	**Aceptable con control específico**
		Fenómenos naturales	**2**	**1**	**2**	**Aceptable**
Mantenimiento preventivo & Correctivo	**X**	**Condiciones de seguridad**	**2**	**2**	**2**	**Aceptable con control específico**

Sistemas de información	**Físico – Eléctrico**	**2**	**1**	**2**	**Aceptable con control especifico**

Fuente: Autores del proyecto.

4.3 Nivel de Madurez FQ Tecnologías

Para identificar el nivel de madurez de TIC en el que se encuentra la empresa FQ Tecnologías, se tuvieron en cuenta varios criterios como adquirir y mantener infraestructura tecnológica, adquirir recursos de TI, Garantizar la continuidad del servicio prestado, garantizar la seguridad de los sistemas y administración del ambiente físico obtenido como resultado que la empresa FQ TECNOLOGÏAS se encuentra en el nivel de madurez de la escala de CMMI.

Tabla 8. *Nivel 2 Tecnología de Información y Comunicación*

TECNOLOGIA DE INFORMACIÓN Y COMUNICACIÓN (TIC)	RECOMENDACIONES
ADQUIRIR Y MANTENER INFRAESTRUCTURA TECNOLOGICA **Decisiones de adquisición** **Sistema configurado para realizar prueba / instalación** **Requerimiento de ambiente físico**	Es necesario ante cualquier cambio de procesos, o instrumentación de nuevas tareas, se debe evitar que los Gerentes y Coordinadores se quejen de que no cuentan con las herramientas necesarias para cumplir con su labor.

Actualización de estándares de tecnología **Requerimiento de monitoreo de sistema** **Conocimiento de la infraestructura**	
ADQUIRIR RECURSOS DE TI **Requerimientos de administración de la relación con terceros** **Proveedores** **Equipos de cómputos**	Se debe incluir la forma de como la organización diseña, controla y mejora sus productos y servicios, incluyendo el enlace con proveedores para construir cadenas que aseguren que los clientes y usuarios reciban valor de forma consistente.
GARANTIZAR LA CONTINUIDAD DE LOS SERVICIOS PRESTADO **Resultados de la prueba de contingencia** **Criticidad de puntos de configuración de TI** **Plan de almacenamiento de respaldos y de protección** **Riesgos** **Requerimientos de servicios contra riesgos incluyendo roles y responsabilidad** **Reportes desempeño de los procesos**	• Administrar todos los proyectos, para el adecuado cumplimiento y entrega final de los proyectos. • Controlar y conocer permanentemente los plazos de entrega de los proyectos. • Cuantificar los resultados, y/o los proyectos realizados.
GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS **Incidentes de seguridad**	• Brindar capacitaciones a los empleados.

Requerimiento especifico de entrenamiento sobre conciencia de seguridad **Reportes de desempeño del proceso** **Cambio de seguridad requeridos** **Amenazas y vulnerabilidad de seguridad**	• Analizar factores actuantes internos y externos.
ADMINISTRACIÓN DEL AMBIENTE FISICO **Reportes de desempeño de procesos**	Diseñar un plan a mediano y largo plazo para el ambiente físico de la empresa, que permita tener una adecuada instalación que logre soportar el área de sistemas e infraestructura TI.

Fuente. Autores del proyecto.

Tabla 9. *Informe de Auditoria FQ Tecnologías*

INFORME DE AUDITORIA FQ TECNOLOGIAS					
TIPO DE AUDITORIA:	**AUDITORIA A PROCESOS**	**VERSIÓN DEL INFORME**	**PRELIMINAR**	**X**	**FINAL**
PROCESO AUDITADO:	Extensión y proyección Tecnológica.				
RESPONSABLE DEL PROCESO:	INGENIERO JAIME FUENTES				

OBJETIVO DE LA AUDITORIA:	Establecer las directrices y lineamientos para planear, ejecutar y evaluar las auditorias de gestión de los procesos de apoyo y de verificación en la implementación de la ISO 27001:2013.
ALCANCE DE LA AUDITORIA:	Desarrollo de un sistema de calidad bajo los lineamientos de la NTC-ISO 27001:2013.
CRITERIOS DE LA AUDITORIA:	La auditoría se realiza según la NTC-ISO 27001:2013.
EQUIPO AUDITOR:	Edgar Muñoz Luis Palmera
AUDITADOS:	Jaime Fuentes – Gerente Jorge Yaguna – Gerente - Coordinador de Proyectos

DESCRIPCIÓN GENERAL DEL DESARROLLO METODOLÓGICO DE LA AUDITORIA

La auditoría al proceso de Extensión y Proyección Tecnológica se desarrolló atendiendo el Plan de Auditoria remitido previamente al Gerente y Coordinadores de Proyectos y fue socializado en reunión de apertura llevada a cabo el día 09 de mayo de 2018. Se describe a continuación la síntesis de ejecución de cada una de las actividades, los hallazgos resultantes tanto positivos como no conformidades se detallan en los aportes. I. FORTALEZAS DEL PROCESO Y/O CONFORMIDADES, II. NO CONFORMIDADES/HALLAZGOS **respectivamente.**

Para la ejecución de la Auditoría en los procesos para la Gestión de Calidad, se lleva a cabo de la siguiente manera:

1. **Reunión de apertura auditoría.**
2. **Presentación del equipo auditor ante el líder del Proceso y/ Procedimiento Auditado.**
3. **Inicio del proceso auditor verificando ciclo PHVA.**
4. **Elaboración de preguntas de acuerdo a la lista de verificación.**
5. **Conclusiones.**

ACTIVIDAD 1: **Revisión de Escritorio: Se solicita a la Oficina de Gerencia la documentación de Planeación vigente del proceso y se reciben los procedimientos vigentes como:**

- ✓ **Verificación de cumplimiento de requisitos bajo las normas ISO 27001:2013**
- ✓ **Verificación de cumplimiento de requisitos legales, técnicos y de oportunidad.**
- ✓ **Verificación del cumplimiento de indicadores y en los diferentes procedimientos.**
- ✓ **Verificación de la Aplicación Acciones Correctivas, Preventivas y de mejoras.**
- ✓ **Verificación del mapa de riesgos y medición de indicadores.**
- ✓ **Solicitud de evidencias objetiva (registros físicos o digitales).**

ACTIVIDAD 2: **Revisión de escritorio: Se solicita Plan Estratégico a Gerencia con el fin de evaluar la Gestión de calidad del Proceso Extensión y Proyección Tecnológica.**

De acuerdo a la revisión realizada, se observa que no existe ningún indicador que mida la gestión de calidad del proceso de Extensión y Proyección Tecnológica.

I. FORTALEZAS DEL PROCESO Y/O CONFORMIDADES:

No.	**Descripción**
1	Las herramientas informáticas con las que cuenta FQ Tecnologías para la Gestión Documental.
2	El compromiso demostrado por todo el personal entrevistado en donde los Lideres de Procesos también manejan sus procesos desde la herramienta de Gestión Documental.
3	Las propuestas de Optimización e Innovación de los Procesos gestionadas por los Lideres de Procesos, apoyados por la Oficina de Gerencia y presentadas al comité de Extensión y proyección Tecnológica.
4	Los recursos Tecnológicos con los que cuenta muestran una empresa sólida en la infraestructura.

HALLAZGOS DE AUDITORIA (NO CONFORMIDADES)

NUMERAL	**REQUISITO**	**DESCRIPCIÓN**	**PROCESO**
4.4	**Sistema de gestión de seguridad de la**	No se evidencia la implementación del sistema de gestión de seguridad de la información y sus procesos a ejecutar,	Gestión de Recursos Tecnológicos.

	información y sus procesos	incumpliendo con los controles establecidos en la norma.	
6.1	**Acciones para abordar Riesgos y Oportunidades.**	No se analiza la eficacia para abordar las oportunidades ; adicionalmente, el análisis para abordar los riesgos en los proyectos de extensión y proyección tecnológica se limita al estado de ejecución de las tareas pero no evalúa la eficacia de las mismas en la reducción o eliminación de los riesgos.	Todos los procesos.
5.3	**Roles, Responsabilidades Y Autoridades En La Organización**	No se evidencian metas para asegurar la medición de los roles, responsabilidades y la eficacia del sistema de gestión de la calidad.	Gestión de Talento Humano.
5.2	**Establecimiento de la política de la calidad.**	No se evidencia una política de gestión de calidad.	Todos los procesos.
5.1	**Liderazgo y Compromiso.**	No se evidencia un compromiso relacionado con la eficacia de los procesos en la gestión de la calidad.	Todos los procesos.
OPORTUNIDADES DE MEJORA			
1	Tener en cuenta los riesgos y los controles al interior de los procesos con el fin de poder cumplir con los objetivos planteados.		

2	Dar aplicabilidad a cada una de las áreas de gestión, como estrategia para el seguimiento y control en los procesos de Gestión de la calidad que hacen parte de la gestión Extensión y Proyección Tecnológica.
3	Incorporar las Normas ISO 27001:2013 a todos los procesos de estratégicos y de apoyo.
4	Fortalecer los ejercicios de planificación de Extensión y Proyección Tecnológica con la construcción de Plan de Acción Vigente, que establezcan una única línea de desarrollo de las necesidades de innovación en los proyectos tecnológicos frente a las necesidades misionales y administrativas.

CONCLUSIONES DE LA AUDITORIA

Fortalezas Identificadas: **3**

Número de No Conformidades: **5**

Número de Observaciones: **4**

Análisis y Recomendaciones Gerencia:

RESPONSABLES

Elaboración y Revisión		**Aprobación**
	Edgar Muñoz	Nombre: Jaime Fuentes
	AL	Nombre: Jorge Yaguna
Equipo	**Luis Palmera**	Cargo: Gerente
Auditor:	**AL**	Firma:

Fecha de elaboración (día/mes/año): 09/05/2018

Fuente. Autores del Proyecto

Tabla 10. *Plan de Mejoramiento FQ Tecnologías*

PLAN DE MEJORAMIENTO FQ TECNOLÓGIAS						
HALLAZGO/ PROBLEMA/ DEBILIDAD	**TIPO DE HALLAZGO (NC / OM)**	**POR QUÉ 1**	**POR QUÉ 2**	**POR QUÉ 3**	**CAUSA RAIZ**	**ACCIONES CORRECTIVAS Y DE MEJORA (Eliminar la causa raíz)**
Tener en cuenta los riesgos y los controles al interior de los procesos con el fin de poder	**OM**	¿Por qué no tiene en cuenta los riesgos y controles en los procesos?	¿Por qué no tenía conocimiento sobre el tema? RTA: no han sido capacitad	¿Por qué no se han capacitado los trabajadores? RTA: la empresa está	Falta de capacitación e información.	Capacitar de manera adecuada al personal de la empresa para prevenir riesgos y tener un control en los procesos.

cumplir con los objetivos planteados.		RTA: por falta de conocimiento sobre el tema.	o los trabajadores de la empresa.	comenzando.		
No se evidencia una política de gestión de calidad.	**NC**	¿Por qué no existe una política de gestión de calidad? RTA: no sabemos en qué consiste la política de calidad.			Falta de información sobre las políticas de calidad existentes.	Asesorarse sobre todas las políticas existentes en Procesos de Gestión de la calidad.
Incorporar las Normas ISO 27001:2013 a todos los	**OM**	¿Por qué no se ha incorporado la norma			Desconocimiento para poder estar certificado.	Investigar e implementar la Norma ISO 27001:2013.

procesos de estratégicos y de apoyo.	ISO 27001:2013 en los procesos estratégicos? RTA: no sabemos cómo poder estar certificados con la norma.				
No se evidencia la implementación del sistema de gestión de calidad en los	¿Por qué no se ha implementado un sistema de gestión de calidad en los	¿Por qué no se han capacitado los empleados?	¿Por qué falta presupuesto en la empresa? RTA: estamos en	Falta de presupuesto empresarial.	Incluir en el presupuesto anual de la empresa las capacitaciones para el personal.

procesos a ejecutar, incumpliendo con los controles establecidos en la norma.	**NC**	procesos a ejecutar? RTA: falta de capacitaciones a los empleados. 	RTA: falta de presupuesto en la empresa.	proceso de incluir el presupuesto para las capacitaciones.		
No se evidencia un compromiso relacionado con la eficacia de los procesos en la gestión de seguridad de la	**NC**	¿Por qué no se verifica la eficacia en los procesos? RTA: no existe un trabajador capacitado para verificar.	¿Por qué no han contratado alguien con experiencia en el tema? RTA: falta de información sobre personal	¿Por qué no se han asesorado sobre el tema? RTA: por ocupaciones diarias de la empresa.	Falta de interés por la empresa, por contratar personal capacitado.	Contratar personal capacitado para mejorar los procesos en la gestión de seguridad de la información.

informació n.	que esté capacitad o para este puesto.		
Auditores:	Edgar Muñoz, Luis Palmera.	**Empresa:**	FQ Tecnológias.

Fuente. Autores del Proyecto

En el desarrollo de la auditoria a los procesos de la empresa se encontraron aspectos que definen el estado actual que presenta la empresa. Por tal razón, se presenta el dictamen de auditoria, el cual describe situaciones encontradas y las recomendaciones por parte de los auditores de acuerdo a los requisitos mínimos exigidos por la NTC ISO 27001:2013 y las buenas practicas con los controles en la NTC 27002.

Donde este dominio trata de mejorar la seguridad en la empresa. En esta auditoria se evaluaron los siguientes aspectos:

Tabla 11. *Objetivos Auditoria*

AUDITORIA			
EMPRESA	**AREA AUDITADA**	**FECHA**	
FQ Tecnologías	Gerencia	15 Junio	2018

OBJETIVO: **Evaluar las vulnerabilidades de la seguridad física y lógica de la información en la oficina de Gerencia de FQ Tecnologías.**

ALCANCE DE LA AUDITORIA: **Identificar los aspectos críticos de la seguridad física y lógica de la oficina de Gerencia de FQ Tecnologías. Y verificar la existencia de controles y acceso a la oficina de Gerencia de FQ Tecnologías.**

RECURSOS: **Al realizar la identificación de los aspectos críticos de la seguridad física y lógica de la oficina de Gerencia de FQ Tecnologías, se identificaron todos los recursos que están en riesgo de vulnerabilidades de la seguridad.**

HARDWARE: **Procesadores, tarjetas, terminales, portátiles, unidades de disco, líneas de comunicación, entre otros.**

SOFTWARE: **Sistemas Operativos, Software libres, Etc.**

DATOS: **Durante la ejecución, almacenados en la nube, archivados fuera de la nube o escritorio remoto, respaldos, base de datos, Etc.**

USUARIOS: **Personas.**

DOCUMENTACIÓN: **De programas, hardware, procedimientos y políticas.**

SUMINISTROS: **Papeles, formularios, medios magnéticos, Etc.**

Tabla 12. SITUACIONES RELEVANTES

OBSERVACIONES	SUGERENCIAS
Hay cajas de corriente eléctrica y enchufes, sin soporte.	Contratar electricista, para mantenimientos preventivos y correctivos.
Los equipos de cómputo no cuentan con numeración de inventario.	Realizar numeración de inventario a cada equipo de cómputo dentro de la empresa.
La actualización de office no se encuentra actualizada.	Mantener actualizadas los paquetes de office y las respectivas licencia.
Los documentos físicos se encuentran en los escritorios de computo.	Ubicar los documentos en cabinas y mantener organizado el escritorio.

Tabla 13. *Situaciones Encontradas*

OBSERVACIONES	SUGERENCIAS
No se encuentra señalización dentro de la empresa que prohíba alimentos y bebidas.	Poner a la vista este informativo.
No existe un Plan de Contingencia.	Realizar un plan de contingencia con colaboración de un agente capacitado, para

	así ponerse de acuerdo con puntos de reunión y salidas de emergencias.
La oficina de Gerencia no está dividida en un cubículo.	Ubicar la gerencia en un cubículo privado para manejar la confidencialidad de la empresa.
El acceso al área de sistemas no es restringido, lo que expone al riesgo a personas, equipos e información.	Controlar el acceso al área de sistemas, con carnets y personal autorizado para ingresar a esta área.
La dependencia no realiza mantenimientos preventivos a los equipos de cómputo.	Realizar mantenimientos preventivos durante un tiempo estipulado, para evitar perdida de información.

4.4 Elementos Del Sgsi Para La Empresa Fq Tecnologías

4.4.1 ISO 27001:2013

Este estándar internacional ha sido para proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

La planificación de un SGSI debe ser una decisión estratégica para la empresa. El diseño e implementación del SGSI de la empresa es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados, el tamaño de la empresa y la estructura de la organización.

El presente Sistema de Gestión de la Seguridad de la Información (SGSI) se basa en la norma ISO 27001:2013, la cual contiene los requisitos básicos que debe tener todo sistema de Gestión de la seguridad de la Información. Se propone un Sistema basado en el Ciclo Deming: Plan, DO, Check Act (Planear, Hacer, Verificar, Actuar), el cual encamina a un sistema de mejora continua con capacidad de adaptarse a cuál entorno empresarial.

Ilustración 14. Ciclo Deming

Fuente: EquipoAltran https://equipo.altran.es/el-ciclo-de-deming-la-gestion-y-mejora-de-procesos/

- **Planificar:** definir la política de seguridad, establecer el alcance del SGSI, Establecer un mapa de procesos, definir autoridades y responsabilidades.

La norma ISO 27001 tiene 11 dominios de controles que cubre los lados más vulnerables o con riesgos de la empresa donde debe existir seguridad de la información, los dominios están divididos en 39 objetivos de control que comprende 133 controles de seguridad para la

empresa. Se seleccionan los controles para planificar el SGSI que aplique la empresa FQ Tecnologías los cuales se encuentran en el Manual de Políticas de Seguridad de la Información.

4.4.2 Fases para un Sistema de Gestión de Seguridad de la Información

- Requerimientos generales
- Establecer y manejar el SGSI
- Monitorear y revisar el SGSI
- Mantener y mejorar el SGSI

4.4.2.1Responsabilidad de la Gerencia. Para la alta gerencia es de vital importancia saber cómo está el clima dentro de la empresa y deben proporcionar evidencia de su compromiso con el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento del SGSI y gestionar todos los recursos que necesite la empresa.

4.4.2.2 Auditorías Internas SGSI.

La empresa debe planear y determinar los objetivos de control, controles, procesos y procedimientos del SGSI que cumplan:

- ✓ Los requerimientos del estándar ISO 27001.
- ✓ Los requerimientos de seguridad de la información identificados.

4.4.2.3 Mejoramiento del SGSI

- ✓ Acción correctiva
- ✓ Acción preventiva

4.5 ISO 27002:2013

El modelo de Seguridad y privacidad de la información en la fase de Planificación se realiza la selección de controles, y durante la fase implementación se ejecuta la implementación de controles de seguridad de la información.

El objetivo de la norma ISO 27002 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones y ser una práctica eficaz de la gestión de la seguridad. Para el desarrollo del Manual de Políticas de Seguridad de la Información base del SGSI, se seleccionó 27002, porque es un marco de trabajo de mejores prácticas internacionales que establece las guías y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en la empresa.

El ISO 27002 contiene 14 Dominios de control de seguridad contenido colección, 35 objetivos de control y 114 controles. Se detallan las diferentes clausulas:

1. **Política de Seguridad de la información**
2. **Organización de la Seguridad de la Información:**
    - ✓ **Organización interna**
    - ✓ **Grupos o personas externas**
3. **Gestión de Activos**
    - ✓ **Responsabilidad por los Activos**
    - ✓ **Clasificación de la información**
4. **Seguridad de Recursos Humanos:**
    - ✓ Antes del empleo
    - ✓ Durante el empleo
    - ✓ Finalización del empleo

5. **Seguridad Física y Ambiental**
    - ✓ Áreas seguras
    - ✓ Equipo de Seguridad
6. Gestión de Comunicaciones y Operaciones
    - ✓ Procedimientos y responsabilidades operacionales
    - ✓ Gestión de la entrega del servicio de terceros
    - ✓ Planificación y aceptación del sistema
    - ✓ Copia de seguridad
    - ✓ Gestión de seguridad de la red
    - ✓ Monitorización
7. **Control de Acceso**
    - ✓ Gestión de acceso del usuario
    - ✓ Responsabilidades del usuario
    - ✓ Control de acceso a la red
8. **Adquisición, Desarrollo y mantenimiento de Sistemas de Información**
    - ✓ Requerimientos de seguridad de los sistemas de información
    - ✓ Procesamiento correcto en las aplicaciones
    - ✓ Controles criptográficos
    - ✓ Seguridad de los archivos del sistema
    - ✓ Seguridad en los procesos de desarrollo y soporte
    - ✓ Gestión de la vulnerabilidad técnica
9. **Gestión de incidentes de Seguridad de la Información**
    - ✓ Informe de los eventos y debilidades de la Seguridad de la información

- ✓ Gestión de los incidentes y mejoras en la seguridad de la información

10. **Gestión de la Continuidad Comercial**

- ✓ Aspectos de la Seguridad de la información de la gestión de la continuidad del negocio

11. **Cumplimiento**

- ✓ Cumplimiento de los requerimientos legales
- ✓ Cumplimiento de las políticas y estándares de seguridad, y cumplimiento técnico

Capítulo 5: Manual de políticas de seguridad de la información

5.1 Alcance

El manual contempla la estructura de gobierno y los lineamientos principales para la seguridad de la información de la empresa FQ Tecnologías. Los lineamientos definidos en este documento deben ser conocidos y cumplidos por empleados, contratistas y todos lo terceros que tengan acceso, almacenen, procesen o transmitan información de la empresa o sus clientes.

Los Gerentes (FQ Tecnologías) deberán revisar y actualizar las políticas de seguridad de la información contenidas en el presente documento una vez al año o cuando los cambios en el entorno lo exijan.

5.2 Organización de seguridad de la informacion

Los gerentes deben identificar las autoridades pertinentes hacia quienes pueda acudir en el caso de que un incidente de seguridad lo amerite. Los gerentes deben de mantener contacto con grupos de interés especial del ámbito de la seguridad de la información que aporten a la gestión de los riesgos de seguridad identificados en la empresa.

En cualquier caso, los proyectos desarrollados por la empresa deben estar alineados a las políticas de seguridad contenidas en el presente manual.

Cada rol dentro de la empresa debe tener unas responsabilidades asociadas para realizar su tarea, estas responsabilidades se asignan a cada rol definido.

Tabla 14. *Roles y responsabilidades*

ROL	REPONSABLES	RESPONSABILIDADES
PROPIETARIO	Gerentes	Serán los responsables de clasificar la información, establecer el nivel de criticidad y disponibilidad de la misma.
RESPONSABLE	Oficina de Extensión y Proyección Tecnológica	Tendrán como responsabilidad asegurar la información de su área, controlando que se cumplan los requerimientos de seguridad de acuerdo con lo indicado por los clientes de la información y las medidas implementadas.
USUARIO	Personas que utilizan el activo de información de manera directa en el día a día dentro de sus funciones laborales o académicas.	Tendrán como responsabilidad hacer buen uso del acceso a la información suministrada para el cumplimiento de sus funciones diarias.

5.3 Seguridad de los recursos humanos

Los siguientes controles están orientados a reducir los riegos de error humano, comisión de ilícitos en el área de tecnología y de sistemas contra el uso inadecuado de instalaciones.

5.4 Antes de asumir el empleo

La oficina de recursos humanos es la encargada de realizar las siguientes actividades relacionadas a la selección del personal administrativo para la empresa y que son fundamentales para la seguridad de la información:

- Verificar los antecedentes de todos los candidatos
- Confirmar la información de referencias personales y familiares, para los casos que el candidato vaya a tener acceso a información considerada sensible para la empresa.
- Como partes de sus términos y condiciones iniciales de empleo, los empleados deberán firmar un compromiso de confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la empresa FQ Tecnologías.

5.5 Durante el empleo

Los gerentes, en razón de proteger la información y los recursos de procesamiento de la empresa, y como demostración de apoyo a la planificación del Sistema de Gestión de Seguridad de la Información, promoverá la cultura de seguridad de la información entre los empleados de la empresa, y por lo tanto expone lo siguiente:

- Promover la importancia de la seguridad de la información entre los empleados e incentivar al cumplimiento de las políticas, normas, procedimientos y estándares establecidos.
- A los casos de incumplimiento al presente manual de políticas de seguridad de la información se le abrirá procesos disciplinarios.

- Asistir a las capacitaciones y actualizaciones periódicas en materia de políticas, normas y procedimientos de la seguridad de la información realizadas por la empresa FQ Tecnologías.
- Todos los empleados serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

5.6 Terminación y cambio de empleo

La empresa FQ Tecnologías asegurará que sus empleados serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura, por lo tanto, se expone lo siguiente:

- La oficina de recursos humanos debe realizar el procedimiento de desvinculación, otorgamiento de licencias, incapacidades, vacaciones o cambio de labores de los empleados de la empresa llevando a cabo los procedimientos que dicha oficina haya establecido.
- Cuando un empleado sea relevado de su cargo en la empresa, el encargado deberá eliminar el usuario y los privilegios de acceso correspondientes al empleado y debe hacer entrega del inventario de activos, credenciales de acceso a su cargo entre otros.

5.7 Gestión de activos

5.7.1 Responsabilidad por los activos de información. La información, los sistemas, los servicios y los equipos de la empresa, son activos de la institución y se proporcionan a los funcionarios y a terceros autorizados, para cumplir con los propósitos de la organización.

- Todos los activos de información deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y criterios.

- Los activos de información de FQ Tecnologías serán identificados, clasificados y valorados para establecer los mecanismos de protección necesarios.
- A los responsables de cada oficina de le brindara las herramientas tecnológicas y complementarias que permitan la administración del inventario garantizado la disponibilidad, integridad y confidencialidad de los datos que lo componen.
- Cada responsable de los activos de información debe monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a información de cada seis meses.
- La oficina de extensión y proyección tecnológica debe establecer un inventario con el software y sistema de información que se encuentran permitidos en los módulos de trabajo de la empresa para el desarrollo de las actividades laborales.
- Si los empleados necesitan instalar, hacer uso o compartir un software (libre o propio), deben solicitar la autorización, verificación y registro del responsable de la oficina.

5.7.2 Documentación de procedimientos operativos. Se debe contar con procedimientos, registros e instructivos de trabajo debidamente documentados y actualizados, con el fin de asegurar el mantenimiento y operación de la infraestructura tecnológica de la empresa. Cada procedimiento debe tener un responsable para su definición y mantenimiento y debe garantizar la disponibilidad del mismo.

5.7.2.1 Eliminación o reutilización de equipos

- Se deben identificar los riesgos potenciales en la empresa que puedan generar, destruir, reparar o eliminar equipos de almacenamiento. Para ello, definir e implementar los mecanismos y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura.

- Cuando un equipo sea reasignado o dado de baja, se deberá realizar un acta donde se ha dado de baja de los inventarios.

5.8 Clasificación de la información

La Gerencia definirá los niveles más adecuados para clasificar su información, de acuerdo con su sensibilidad y la oficina de extensión y proyección tecnológica generará una Guía de clasificación de la información para que la Gerencia catalogue y determine los controles requeridos para su protección.

Toda la información debe ser identificada, clasificada y documentada de acuerdo con la guía de clasificación de la empresa con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos.

5.8.1 Tratamiento de la información de Titulares

- Garantizar el derecho de habeas data.
- Almacenar la información de forma segura impidiendo que sea adulterada, perdida, consultada sin previa autorización.

5.8.2 Acceso a internet

La compañía provee el servicio de internet para empleados, proveedores, contratistas, clientes y terceras partes que se encuentran dentro de las instalaciones, requieran de la prestación de este servicio de manera controlada, se deben seguir los siguientes criterios:

No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.
- El intercambio no autorizado de información de propiedad de la empresa, de sus clientes, usuarios y/o funcionarios, con terceros.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de los usuarios, o que contengan archivos ejecutables.
- La empresa debe monitorear los tiempos de navegación y páginas visitadas por parte de los funcionarios, contratistas y/o terceros.
- Cada uno de los empleados es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas.
- Los empleados, contratistas y terceros o subcontratistas de estos, no pueden asumir en nombre de la empresa, posiciones personales encuestas de opinión, foros u otros medios de comunicación externos similares.
- El uso de internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la empresa.
- El servicio de internet esta designado para el uso laboral.
- La empresa se reserva el derecho de filtrar el contenido al que el usuario puede acceder a través de internet.

- Por motivos de seguridad y para evitar el contagio de virus, se prohíbe la descarga de software desde internet.

5.8.3 Correo Electrónico

- Las cuentas de correo electrónico deben ser usada para el desempeño de las funciones asignadas dentro de la empresa.
- Los mensajes e información contenida en los correos son propiedad de la empresa y del responsable encargado, solo deben mantener los mensajes relacionados con el desarrollo de sus funciones.
- El correo electrónico corporativo es la única vía de remisión o envió de documentos de carácter administrativo interno en la empresa.

No está permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racistas, sexistas, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de los usuarios o clientes.
- Enviar mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
- Interactuar por medio del correo electrónico con comunidades de contacto social, tales como Facebook, Instagram, twitter entre otras.
- Él envió de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

5.9 Acuerdos sobre confidencialidad

- Todos los empleados de la empresa FQ Tecnologías, contratistas, clientes o terceros que presten servicios deberán aceptar los acuerdos de confidencialidad definidos por la

institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en el manual.

- Para los contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad; en caso de incumplirla se dictarán los respectivas acciones legales y debidos procesos.
- Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula o acuerdo de confidencialidad hace parte integral de cada uno de los contratos realizados por la empresa FQ Tecnologías.

5.10 Clasificación de la información

La guía de clasificación de la información define los controles técnicos y administrativos que se implantarán en la empresa con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos en función de su nivel de clasificación.

- La empresa con el fin de resguardar la información que pueda ser divulgada de forma no autorizada o manipulada erróneamente por parte de sus empleados, contratistas, proveedores o clientes.
- Toda la información de la empresa debe ser identificada, clasificada y documentada de acuerdo con los criterios de clasificación establecidos por el comité de gerencia de la información.
- Verificar las áreas cercanas a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no queden documentos relacionados.
- Los empleados deben asegurar que los documentos y medios de almacenamiento que contengan información sensible, no queden de forma desprotegida en el momento de ausentarse de su puesto de trabajo.

- Para cumplir con la clasificación a continuación se presentan los tipos de prioridad para la información:

✓ Publica: estará la información que se pueda compartir.

✓ Uso interno: estará la información de interés para la empresa, en general.

✓ Información confidencial: estará la información de interés solo para un área en particular o por disposición de la ley (Información sensible, privados, menores de edad, etc.).

✓ Los gerentes deben resguardar la información almacenada en medios magnéticos, de carácter histórico, esta quedará documentada como activo del área.

✓ Ningún empleado de la empresa o tercero debe posees material o información confidencial de la empresa, para usos no propios de su responsabilidad.

5.10.1 Etiquetado de la información

La información almacenada en medios magnéticos se debe inventariar, anexando la descripción y las especificaciones de la misma, clasificándola y etiquetándola en los mismos niveles establecidos en clasificación de la información.

Los responsables de los activos de información clasificadas deben identificar y asociar el nivel de clasificación a cada activo, teniendo en cuenta los criterios de clasificación, y su protección se establece de acuerdo con lo definido en el inventario de activos de información de la empresa.

5.11 Seguridad física y de entorno

Áreas Seguras

- La protección de los activos de la empresa se llevará a cabo mediante la creación de cubículos o perímetros de seguridad en las instalaciones de la empresa que contengan información confidencial o critica.

- Las áreas que estén protegidas se resguardarán mediante el empleo de controles de acceso físico y protección los que serán determinados por los gerentes, a fin de permitir el acceso sólo al personal autorizado.
- Se tendrá en cuenta la posibilidad de daño o riesgo producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre.
- Se tomarán disposiciones y aplicarán normas generales en materia de sanidad y seguridad.

Equipos

- Los activos de la empresa serán ubicados y protegidos de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales.
- El suministro de energía funcionará de acuerdo con las especificaciones de los proveedores de cada equipo.
- El cableado de energía eléctrica y de telecomunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegida contra intercepción o daño.
- Se implementará un plan de mantenimiento preventivo y correctivo para los equipos y velará por el cumplimiento del mismo.
- Los cubículos de trabajo deben estar correctamente asegurados.
- Los equipos que hacen parte de la infraestructura tecnológica de la empresa tales como equipos de comunicación y seguridad electrónica, centros de cableado, UPS, aires acondicionados, entre otros, deben ser ubicados y protegidos adecuadamente para prevenir, daño, robo o acceso no autorizado de los mismos.

Controles de acceso físico

- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran área de acceso restringido.
- De igual manera, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.).
- En caso de retiro o desvinculación laboral del funcionario, contratista o tercero, este debe hacer devolución de la respectiva escarapela asignada en desarrollo de sus funciones, previa liquidación de sus prestaciones sociales y demás obligaciones.

Gestión de Contraseñas

- El administrador de cada sistema de información es responsable debe asegurar que este solicite usuario y contraseña para permitir el acceso.
- El administrador de cada sistema es responsable de asegurar que este solicite cambio de contraseña cada un mes cumplido.
- La contraseña debe estar compuesta por una combinación de letras, Mayúsculas, minúsculas, caracteres numéricos y símbolos especiales como los siguientes: ñ, ¡, !, @, #, $, %, &, entre otras.
- No deben utilizarse contraseñas como fechas de cumpleaños, cedula, nombre de familiares.
- Las aplicaciones deben almacenar las contraseñas en forma cifrada.
- Las contraseñas predefinidas que traen los equipos deben cambiarse inmediatamente.

- Las contraseñas deben cambiarse cuando una persona es relevada de su cargo.

Uso de los recursos compartidos en la Red

Los empleados, proveedores, contratistas, clientes y terceros que tengan acceso a los recursos compartidos de la compañía deben cumplir con los siguientes criterios:

- Es responsabilidad de la oficina de Extensión y Proyección Tecnológica asegurar que el acceso a la red (inalámbricas y físicas) para el uso de recursos compartidos.
- No es permitido intercambiar o guardar archivos de audio (Wav, mp3, etc.).
- No es permitido almacenar información de la compañía en medios públicos de almacenamiento en la nube no autorizados por la empresa.
- Todo empleado debe validar con los gerentes antes de eliminar cualquier información del recurso compartido.
- Se debe guardar únicamente información relacionada con las funciones de su cargo.

5.12 Protección de datos personales

La empresa FQ Tecnologías da cumplimiento a las normas de protección de datos personales definidos en la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas que lo complementan, así como al Manual de Tratamiento de Datos que se ha adoptado para el efecto.

5.12.1 Propiedad Intelectual.

Los empleados son responsables de respetar y dar cumplimiento a las disposiciones legales de derechos de autor, marcas registradas y derechos de propiedad intelectual para toda la información que se instala, copia o descarga de internet para la empresa.

5.13 Gestión de vulnerabilidades técnicas

La Oficina de Extensión y Proyección Tecnológica es responsable de:

- Identificar, valorar, revisar y gestionar las vulnerabilidades técnicas del sistema de información críticas, con el objetivo de realizar la corrección sobre los hallazgos arrojados.
- Verificar por lo menos una vez cada trimestre la información y foros de seguridad en relación con nuevas vulnerabilidades identificadas que puedan afectar el sistema de información de la empresa.
- Generar anualmente un plan de pruebas de vulnerabilidades para las plataformas criticas del negocio.
- Implementar los correctivos que requieran ser aplicados en las plataformas tecnológicas, derivados de la identificación de vulnerabilidades técnicas.

Desarrollo Seguro

La Oficina de Extensión y Proyección Tecnológica de asegurar que los desarrollos internos y externos de los Sistemas de Información cumplan con los requisitos definidos, con las buenas prácticas para el desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software.

- Se asegurará que todo software desarrollado interna o externamente cuente con el soporte requerido.

Los desarrolladores de los Sistemas de Información deben considerar las siguientes prácticas:

- **Principio del Menor Privilegio:** las cuentas de usuario deben tener la menor cantidad de privilegios para llevar a cabo sus actividades.

- **Seguridad por defecto:** todos los accesos que se hagan a los sistemas deben estar validados, el sistema debe exigir la complejidad y cambio de contraseñas periódicamente:
- **Defensa en Profundidad:** proteger con más de un mecanismo de defensa la base de datos los cuales contienen información sensible.
- **Manejo adecuado de errores:** se debe utilizar mecanismos de manejo de errores ripo try catch con el fin de publicar la información mínima requerida.
- **Validación de datos de entrada:** todos los datos de entrada de la aplicación deben ser verificados y sanitizados.
- **Criptografía:** intercambiar información sensible utilizar protocolos para citar las comunicaciones, y en el caso de almacenamiento de información confidencial debería estar cifrada.
- **Control de cambios:** cualquier cambio que se haga deberá quedar documentado, eso facilitara modificaciones futuras.
- **Manejo de Logs:** las aplicaciones deben dejar rastro para el seguimiento de las principales actividades realizadas por los usuarios, por ejemplo: actividades de autenticación, de inserción, y de modificación de base de datos.
- **Gestión de Vulnerabilidad Técnica:** hacer un seguimiento de las tecnologías utilizadas para el desarrollo.
- **Manejo de Sesiones:** se deben implementar medidas de manejo de sesión que mitiguen los principales ataques: predicción de sesión o secuestro de sesión.
- **Pruebas de Seguridad y Aceptación:** todo desarrollo realizado deberá contemplar las pruebas de seguridad y de aceptación dependiendo del tipo de proyecto (Corte o

robustecimiento de producto lo acepta el Gerente o si es proyecto de un cliente, el cliente es quien aprueba el cumplimiento de estos requisitos).

COPIAS DE RESPALDO

- Los medios que alojan copias de seguridad deben estar correctamente conservados de acuerdo a las políticas y estándares definidos por los Gerentes de la empresa.
- Se elaborará copias de seguridad diarias a los sistemas de información y las guardará en sitios bajo llave en la oficina.
- Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta.
- El sitio externo donde se resguardan dichas copias, debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

GESTIÓN DE INCIDENTES

Eventos aleatorios, causados por el hombre o por la naturaleza, previsibles o no, tales como el terrorismo, terremotos, entre otros eventos, pueden generar interrupciones a la empresa en la entrega de productos y servicios. Los lineamientos establecidos para la Gestión de continuidad del negocio tienen como fin, seguir entregando los productos y servicios a un nivel aceptable y este permitirá:

- Resolver los incidentes de manera sistemática, eficiente y rápida.
- Estar preparado ante cualquier incidente inesperado con el fin de volver a la normalidad en poco tiempo.
- Evitar al máximo la perdida de información.
- Trabajar continuamente por mejorar en la gestión y tratamiento de incidentes.

- Generar una base de datos donde se guarde una línea de tiempo sobre incidentes en la empresa.
- Evitar al máximo, incidentes repetitivos.

Reportes de Incidentes de Seguridad Informática

Se debe para cualquier incidente de la empresa a los Gerentes, diligenciados y manifestando las causas del incidente y del empleado que reportó:

Tabla 15. *Reporte De Incidentes*

REPORTES DE INCIDENTES		
Datos del reporte de incidencia		
Número:	Fecha:	Hora:
Descripción del incidente:		
Efectos producidos:		
Responsable del activo afectado:		
Causa del incidente:		
Nombre y Apellido:		
Cargo:		
Dependencia:		
Correo:		

- Todos los empleados que son usuarios de los sistemas y servicios de la empresa deben anotar y comunicar cualquier debilidad observada o sospechada en la seguridad.

- El empleado o encargado de reportar el incidente puede hacerse las siguientes preguntas:
    - ✓ ¿Cuántos activos de la empresa fueron afectados?
    - ✓ ¿Qué es lo que más está en riesgo?
    - ✓ ¿Cuán conocida es la vulnerabilidad explotada por el atacante?
    - ✓ ¿hay otros activos con la misma vulnerabilidad?
- La contención, evitara que el incidente siga produciendo daños.
- La erradicación eliminara la causa del incidente.
- La recuperación consiste en volver el entorno afectado a su estado original.

Conclusión

Después de haber llevado a cabo el diagnóstico de la oficina de Extensión y Proyección Tecnológica de FQ Tecnologías a través de una auditoria interna con la norma ISO 27001:2013, logramos alcanzar el conocimiento suficiente sobre cómo se encuentra los elementos corporativos como la misión, visión, y organigrama dentro de la empresa. El estudio realizado demostró que la oficina no cuenta con la formulación de estos elementos y en algunos casos la inexistencia de los mismos objetivos; razón por la cual se realiza una propuesta de misión, visión, objetivos, organigrama e procesos misionales.

Con este proyecto de grado se Planifico un Sistema de Gestión de Seguridad de la Información para la empresa FQ Tecnologías, basado en la norma ISO 27001:2013. Se realizaron varios diagnósticos que permitieron establecer el nivel de madures de la empresa frente a la gestión de la seguridad de la información. En una primera fase se obtuvo un diagnostico a partir de varias auditorías realizadas, analizando tanto a los empleados y procesos de Gestión de la Información, como a los activos físicos, técnicos, tecnológicos que se encuentran dentro de la empresa.

A partir de esto, se creó un Manual de Políticas de Seguridad de la Información que será beneficioso para la empresa en cuanto a: seguridad efectiva en los sistemas de información; mejoras continuas en procesos de auditorías internas dentro de la empresa; incremento de confidencialidad, confianza y responsabilidad en los procesos.

Recomendaciones

Es necesario que se tenga en cuenta el ciclo de vida de los activos de información, ya que lo que puede ser crítico hoy para la empresa puede dejar de tener importancia con el tiempo.

Es de gran importancia el compromiso de la Gerencia, la revisión y actualización anual del Manual de Políticas de Seguridad de la Información.

Se recomienda que la empresa elabore planes que permitan realizar un seguimiento constante a los roles diseñados y del cumplimiento de las responsabilidades de cada encargado en la empresa.

Generar planes de capacitación y controles que involucren a todas las partes externas, las cuales deben garantizar la confiabilidad, integridad y disponibilidad de la información, por medio del cumplimiento de la normatividad y leyes vigentes.

Referencias

Cárdenas Herrera, C., & Higuera Soto, D. (2016). *Diseño de un Sistema integrado de Gestión basado en las normas ISO 9001:2015 e ISO 27001:2013 para la empresa la casa del Ingeniero LCI.* Bogotá: Escuela Colombiana de Ingeniería Julio Garavito.

Casadiegos Santana, A., Quintero Jiménez , M., & Toro Rueda, M. (2012). *Sistema de Gestión de Seguridad de la Información para el área de contabilidad de la E.S.E Hospital Local de Rio de Oro Cesar*. Ocaña: Universidad Francisco de Paula Santander.

Castilla Vergel, G., Echaves Casadiegos, G., Rodriguez Osorio, J., & Sandoval Sanjuan , D. (2014). *Sistema de Gestión de Seguridad de la Información para la oficina de Control y Vigilancia en la Corporación Autonoma de la Frontera Nororiental "Corponor" Territorial Ocaña.* Ocaña: Universidad Francisco de Paula Santander Ocaña.

Doria Corcho, A. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información mediante la Aplicación de la Norma Internacional ISO/IEC 27001:2013 en la Oficina de Sistemas de Información y Telecomunicaciones de la Universidad de Córdoba.* Montería: Universidad Nacional Abierta y a Distancia.

Gerrero Melo, J., & Suarez Castrellon, F. (2012). *Planeación del Sistema de Gestión de Seguridad de la Información aplicando la Norma Internacional ISO/IEC 27001:2013 en*

área contable en la empresa transformadores CDM. Ocaña: Universidad Francisco de Paula Santander Ocaña.

Gómez Fernandez, L., & Álvarez , A. (2018). Guíz de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad de información para Pymes. *https://s3.amazonaws.com/academia.edu.documents/36974512/NOV_DOC_Tabla_AEN_22994_1.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1528734560&Signature=gmGSHg6MPwJun9xjugrmJEjvlj4%3D&response-content-disposition=inline%3B%20filename%3DNOV_DOC_Tabla_AEN_22*. Obtenido de https://s3.amazonaws.com/academia.edu.documents/36974512/NOV_DOC_Tabla_AEN_22994_1.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1528734560&Signature=gmGSHg6MPwJun9xjugrmJEjvlj4%3D&response-content-disposition=inline%3B%20filename%3DNOV_DOC_Tabla_AEN_22

González Agudelo, D. (2014). El Riesgo y la Falta de Politicas de Seguridad Informática una Amenaza en las Empresas Certificadas BASC. En *El Riesgo y la Falta de Politicas de Seguridad Informática una Amenaza en las Empresas Certificadas BASC* (pág. 24). Bogotá: Universidad Militar Nueva Granada.

Guzman Silva, C. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Financiera de Segundo Piso.* Bogota: Institución Universitaria Politécnico GranColombiano.

Guzman Silva, C. (2015). *Diseño de un Sistema de Gestión de seguridad de la Información para una Entidad Financiera de Segundo Piso.* Bogota: Institución Universitaria Politecnico GranColombiano.

Lievano Cos, F. (2016). *Sistema de Gestión de la Seguridad de la Información.* España: Universidad Oberta de Catalunya.

MINISTERIO DE DEFENSA NACIONAL . (2016). Resolución Número 08310 de 28 Dic 2016. En P. NACIONAL. Bogotá.

MINISTERIO DE EDUCACIÓN NACIONAL. (2018). Resolución Número 01760 de 09 FEB 2018. Bogota.

Ministerio de Tecnologías de la información y las comunicaciones . (2014). Decreto Número 2573 de 2014. Bogotá.

MINTIC. (s.f.). Seguridad y Privacidad de la Información. En *Modelo de Seguridad y Privacidad de la Información* (pág. 58). Bogotá: Vive Digital.

Oficina TIC Los Patios. (2017). *Manual de Normas y Políticas de Seguridad de la Información.* Ocaña: Alcaldía Municipio de los Patios.

Rodríguez Correa, J. (2017). *Diseño de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en ISO 27001 para laboratorios servicios farmaceuticos de calidad SFC LTDA.* Bogotá: Universidad abierta y a distancia - UNAD.

Santiago, E., & Sánchez Allende, J. (2017). RIESGOS DE CIBERSEGURIDAD EN LAS EMPRESAS. *Revista Tecnologí@ y Desarrollo*, 33.

SIGEPRE. (2018). *MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN*. Bogotá: SIGEPRE.

Solarte Solarte, F., Enriquez Rosero, E., & Benavides Ruano, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL, 28*(5), 16. Obtenido de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

TUV SUD. (2013). ISO/IEC 27001 Gestión de Seguridad de la Información. *TUV-SUD*, 2.

Valls, M. (2017). ESTRATEGIA NACIONAL FRANCESA PARA LA SEGURIDAD DEL ÁMBITO DIGITAL. En *ESTRATEGIA NACIONAL FRANCESA PARA LA SEGURIDAD DEL ÁMBITO DIGITAL* (pág. 44). Francia: PREMIER MINISTRE.

Apéndices

Apéndice A: Papeles de trabajo de la auditoria

REPORTE DE PRUEBAS Y RESULTADOS					
	EMPRESA	**AREA AUDITADA**	**FECHA**		
	FQ TECNOLOGÍAS	Gerencia	15	06	2018
Objetivo: Verificar la seguridad lógica y seguridad de FQ Tecnologías.					

PRUEBA N°1

GERENCIA FQ TECNOLOGÍAS – VALLEDUPAR

Prueba	Seguridad Física de la Oficina de Gerencia
Objetivo	Verificar las Condiciones de Seguridad de la Oficina de Gerencia.
Técnica	Lista de chequeo - Observación
Tipo de Prueba	Cumplimiento Sustantiva X Doble Finalidad
Procedimiento a Emplear	Utilizar la Observación y Entrevista como herramienta para verificar el estado Físico donde se encuentran ubicados los equipos.
Recursos	Humanos, Equipos, Documentación Física.

RESULTADOS DE LA PRUEBA

Hallazgos	La oficina de Gerencia está expuesta a todo el personal que entra a FQ Tecnologías por lo cual su acceso no es controlado y se permite el consumo de alimentos cerca de los aparatos de computo.
Causa	La Gerencia no se encuentra ubicada en un cubículo con acceso restringido. No existen avisos o restricciones para consumir alimentos dentro de la oficina de Gerencia.
Situación de Riesgo que genera	Manipulación de los equipos de la oficina de Gerencia. Perdida o daño de los equipos de la oficina de Gerencia.
Recomendaciones de Auditoria	Con el fin de Prevenir actos criminales o en su defecto tener registro de dicho acto se recomienda realizar la inversión para ubicar la oficina de Gerencia en un cubículo independiente que tenga puerta con cerradura y llave que limite el acceso a personal autorizado únicamente.
Fecha	02 julio 2018
Elaborado por	Edgar Muñoz
Revisado por	Luis Palmera

PRUEBA N°2

FQ TECNOLOGÍAS - VALLEDUPAR

Prueba	Seguridad de Inventario de Hardware

Objetivo	Verificar los controles para proteger los Hardware existentes dentro de la oficina.
Técnica	Lista de Chequeo – Observación
Tipo de Prueba	Cumplimiento Sustantiva Doble Finalidad X
Procedimiento a Emplear	Aplicar lista de chequeo con el fin de verificar los controles a la seguridad de Hardware. Visita a la Organización con el fin de observar la aplicación de controles en la seguridad de Hardware dentro de la oficina de Gerencia.
Recursos	Humanos, Equipos de cómputo.
RESULTADOS DE LA PRUEBA	
Hallazgos	Se evidenció que no existen controles eficientes para evitar algún suceso con los equipos o Hardware dentro de la oficina.
Causa	Perdida o extravió eventual de los equipos de cómputo sin alguna causa.
Situación de Riesgo que genera	Perdida de activos dentro de la oficina de Gerencia.
Recomendaciones de Auditoria	Se recomienda elaborar un inventario general de los equipos de cómputos o activos dentro de la oficina de Gerencia para prevenir actos delictivos.
Fecha	03 julio de 2018
Elaborado por	Luis Palmera
Revisado por	Edgar Muñoz

PRUEBA N°3	
FQ TECNOLOGÍAS - VALLEDUPAR	
Prueba	Plan de Emergencia
Objetivo	Verificar los Planes de Emergencia que implementan dentro de la oficina de Gerencia.
Técnica	Lista de Chequeo – Observación
Tipo de Prueba	Cumplimiento Sustantiva Doble Finalidad X
Procedimiento a Emplear	Aplicar lista de chequeo con el fin de verificar los planes de emergencia existentes dentro de la oficina de Gerencia. Visita a la Empresa con el fin de observar la aplicación de los planes de emergencia.
Recursos	Humanos, Gerencia, Contabilidad.
RESULTADOS DE LA PRUEBA	
Hallazgos	Se evidenció que no existen planes de emergencias eficientes en caso de alguna catástrofe.
Causa	Todo personal que tenga acceso a la dependencia de FQ Tecnologías, no identifica que hacer en caso de una emergencia.
Situación de Riesgo que genera	Desubicación del personal al momento de una catástrofe.
Recomendaciones de Auditoria	Asignar un plan de emergencia adecuado con señalización o en su defecto tener un personal idóneo para realizar el trabajo.

Fecha	04 julio de 2018
Elaborado por	Edgar Muñoz
Revisado por	Luis Palmera

PRUEBA N°4

FQ TECNOLOGIAS - VALLEDUPAR

Prueba	Circuitos Eléctricos
Objetivo	Verificar el control preventivo a los circuitos eléctricos.
Técnica	Lista de chequeo – Observación
Tipo de Prueba	Cumplimiento Sustantiva X Doble Finalidad
Procedimiento a Emplear	Verificar el cableado eléctrico de la oficina de Gerencia.
Recursos	Equipos de cómputo, circuitos eléctricos.

RESULTADOS DE LA PRUEBA

Hallazgos	No se tiene programación para realizar mantenimientos preventivos a los circuitos eléctricos dentro de la oficina de Gerencia.
Causa	Solo se hace mantenimiento correctivo, al momento de ocurrir un corto circuito.
Situación de Riesgo que genera	Pérdida de tiempo y dinero, en lo que respecta un daño importante dentro de la oficina de Gerencia.
Recomendaciones de Auditoria	Se les da a conocer la importancia de hacer una programación de mantenimientos preventivos a la oficina de gerencia, ya que disminuye los costos de un

	mantenimiento correctivo y logra que se trabaje de manera eficiente diariamente.
Fecha	05 julio de 2018
Elaborado por	Luis Palmera
Revisado por	Edgar Muñoz

LISTA DE CHEQUEO HOJA 1/2

EMPRESA/AREA	**RESPONSABLE**	**FECHA**		
FQ TECNOLOGÍAS	GERENCIA	02	07	2018

Objetivo: **Conocer los controles existentes en cuanto a la seguridad física del hardware, de la gerencia de FQ TECNOLOGÍAS.**

No	**Preguntas**	**Cumple**	**No Cumple**	**Observación**
	A. Acceso físico			
1	¿Existen mecanismos de identificación al personal que ingresa a la gerencia?		**X**	No existe algún mecanismo para identificar el
2	¿Existe localización y señalización adecuada de áreas sensibles?		**X**	ingreso a gerencia.

3	¿La ubicación de la oficina de gerencia es independiente de otras oficinas y es la adecuada?	**X**	No están señalizadas las áreas sensibles. La oficina de gerencia se comparte con la oficina de contabilidad.
	B. Inventario Hardware		
5	¿Se encuentra inventariado el hardware que reposa en la Gerencia?	**X**	No se encuentra inventariado los Hardware dentro de la Gerencia.
6	¿Cada dispositivo o periférico tiene la numeración respectiva del inventario?	**X**	
7	¿Existe personal autorizado para controlar la salida de dispositivos del área de la dependencia?	**X**	No existe numeración para los dispositivos.
8	¿Tiene conocimiento de algún faltante del inventario de hardware como	**X**	No hay personal idóneo, para verificar la

9	periféricos, equipos de cómputo o algún dispositivo?	**X**	salida de los dispositivos.
	¿Se realizan mantenimientos preventivos a los dispositivos de cómputo?		No se realizan mantenimientos preventivos, periódicamente.
	C. Plan de Emergencia		
11	¿Cuentan con un plan de Emergencia?	**X**	No existe dentro de la empresa un
12	¿Existen planes y manuales sobre normas de actuación en caso de emergencia?	**X**	plan o mecanismo de emergencia para
13	¿Existe señalizacion para la evacuacion en caso de una emergencia dentro de la empresa?	**X**	contrarrestar alguna catastro.
14		**X**	
15	¿Se realizan simulacros de emergencia para saber cómo actuar y qué hacer con los dispositivos en caso de que ocurra una eventualidad?	**X**	

	¿Existen salidas de emergencias?		
	D. Circuitos Eléctricos		
16	¿Tienen contrato con algún electricista para que revisen las instalaciones eléctricas?	**X**	No hay un personal adecuado para las reparaciones o mantenimientos preventivos en los circuitos eléctricos dentro de la empresa.
17	¿Se revisan los circuitos eléctricos dentro de la empresa?	**X**	
18	¿Los circuitos eléctricos y el cableado cumplen con los estándares?	**X**	
19	¿Se han generado cortos circuitos en la empresa?	**X**	
20	¿Hay extintores en puntos clave de la empresa?	**X**	
21			

¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?

II INVENTARIOS

DEL	**02**	**07**	**2018**
AL	**07**	**07**	**2018**

INVENTARIO DE HARDWARE

PERIODO: 02 AL 07 DE JULIO

EMPRESA: FQ TECNOLOGIAS

AUDITOR:

#	EQUIPO	MARCA	NÚM. INVENTARIO	CARACTERISTICAS	OBSERVACIONES
01	Computadores	Acer	9	E5-475	Portátiles
02	Computadores	Lenovo	2	Yoga 520-14ikb	Portátiles
03	monitor	Samsung	2	Cf391	
04	impresora	Samsung	2	M2070fw	
05	Router	Tp-link	1	Tl-wr941hp	
06	Silla gerencial		11	Silla gerencial	
07	Escritorios oficina		8	escritorio oficina	

08	**Mesa de juntas**		**1**	**Mesa de juntas**	**La mesa viene con 4 sillas**
09	**Aire acondicionado**	**Mabe**	**2**	**Aire mabe invertir 9000 btu 220v**	
10	**Kit Cámara de seguridad**	**Hikvison**	**1**	**Dvr turbo hd 8ch**	**2 cámaras tipo bala 6 cámaras tipo domo**

02	**07**	**2018**
07	**07**	**2018**

DEL

AL

EMPRESA: FQ TECNOLOGÍAS

PERIODO: 02 AL 07 DE JULIO

RESPONSABLE:

INVENTARIO DE SOFTWARE							
REF	**SOFTWARE**	**VERSIÓN**	**NÚM. INVENTARIO**	**LICENCIAS**	**PRESENTACIÓN**	**ASIGNADO A**	**LOCALIZACIÓN**
O01	**OFFICE**	**2017**		**1**	**CD-ROM**	**CONTABILIDAD**	**FINANZAS**
O02	**OFFICE**	**2017**		**1**	**CD-ROM**	**AUXILIAR CONTABLE**	**FINANZAS**
O03	**OFFICE**	**2017**		**1**	**CD-ROM**	**SECRETARIA**	**R. HUMANOS**
O04	**OFFICE**	**2017**		**1**	**CD-ROM**	**AUXILIAR ADMIN**	**R. HUMANOS**

O05	**OFFICE**	**2017**		**1**	**CD-ROM**	**DIRECTOR DE PROYECTO 1**	**DESARROLLO**
O06	**OFFICE**	**2017**		**1**	**CD-ROM**	**DIRECTOR DE PROYECTO 2**	**DESARROLLO**
O07	**OFFICE**	**2017**		**1**	**CD-ROM**	**DIRECTOR DE PROYECTO 3**	**DESARROLLO**
O08	**OFFICE**	**2017**		**1**	**CD-ROM**	**GERENCIA**	**DESARROLLO**
O09	**OFFICE**	**2017**		**1**	**CD-ROM**	**DESARROLLADOR 1**	**DESARROLLO**
O010	**OFFICE**	**2017**		**1**	**CD-ROM**	**DESARROLLADOR 2**	**DESARROLLO**
O011	**OFFICE**	**2017**		**1**	**CD-ROM**	**DESARROLLADOR 3**	**DESARROLLO**
W01	**WINDOWS 10**	**2018**		**11**	**CD-ROM**	**GERENCIA**	**ADMOS**
V01	**VISUAL**	**2015**		**FREE**	**CD-ROM**	**DESARROLLADORES**	**DESARROLLO**

	STUDIO						

ENTREVISTA DIRIGIDA A LA GERENCIA DE FQ TECNOLOGIAS					HOJA 1/2
	EMPRESA	AREA AUDITADA	FECHA		
	FQ Tecnologías	Gerencia	02	07	2018
Objetivo: Indagar sobre la seguridad de la información en la empresa FQ Tecnologías					
Funcionario entrevistado: Mayra Vanegas		Cargo: Gerente			
Inicio de la entrevista con saludo y explicación breve de objetivo de la entrevista.					

AUDITOR: Por favor comente cuantas personas laboran en la empresa, y si están completamente capacitadas para ejercer el cargo que desempeñan.

GERENTE: En la empresa trabajan 11 personas de las cuales Todas se encuentran Capacitadas para realizar su labor, periodica mente enviamos a nuestros Trabajadores a Capacitaciones para reforzar su Conocimien

AUDITOR: De qué manera se maneja la documentación legal en la empresa, al momento de registrar toda la información.

GERENTE: Toda la documentación legal se maneja en archivos fisicos

AUDITOR: De qué manera se le da a conocer al personal sus funciones, responsabilidades y la forma de realizar sus actividades.

GERENTE: Esta información se le proporciona a los empleado de forma verbal, amedida que se realizan nuevos proyectos

AUDITOR: Que tanta antigüedad tienen los equipos con los que cuentan la empresa actualmente, estos equipos permiten el logro de los objetivos para el personal de la empresa.

GERENTE: los equipos con los que cuenta la empresa fueron comprados en el año 2014 los cuales nos han permitido cumplir todos nuestros proyectos y demas labores hasta la fecha

AUDITOR: Hasta la fecha cuantos proyectos existen en la empresa, que generan mayor impacto de innovación, calidad e investigación a nivel departamental.

GERENTE: Hasta la fecha resaltan 7 proyectos a nivel departamental, realizados pra entidades del estado y empresas prestadoras de servicios importantes de la region, con el fin de optimizar sus procesos

AUDITOR: Actualmente cuenta con un plan estratégico, donde estén establecidos los procesos Misionales y/o de apoyo.

GERENTE: Se cuenta con el desde la constitucion legal de la empresa en el se incluye: mision, vision, objetivo estrategicos y reglamentos institucionales

AUDITOR: Explique el proceso y la frecuencia con que se hace respaldo de la información. Además, enuncie el o los responsables de realizarlos.

GERENTE: Se llevan acabo 2 tipos distintos de información 1. respaldo en la nube que se hace semanal de forma automatica y el un respaldo fisico que se hace mensual en los discos duros propios de la empresa

AUDITOR: Actualmente cuenta con un Sistema de información en la empresa y quien es el responsable del mismo. En caso de que cuente con uno, cómo se realiza el acceso al Sistema de información existente en la empresa y que controles de seguridad se tienen para dicho acceso.

GERENTE: no se cuenta con un Sistema de informacion, Todos los procesos Contables y administrativos se manejan en hojas de Calculo en microsoft excel

ENTREVISTA DIRIGIDA A LA GERENCIA DE FQ TECNOLOGIAS					HOJA 1/2
	EMPRESA	AREA AUDITADA	FECHA		
	FQ Tecnologías	Gerencia	02	07	2018
Objetivo: Indagar sobre la Seguridad Física y Seguridad de la Información de la empresa FQ Tecnologías.					
Funcionario entrevistado: todo el personal de la empresa.		Cargo: contador. Coordinador de Proyectos, auxiliar de archivo, Gerencia, Secretaria ejecutiva			

I. INFRAESTRUCTURA

EVALUACION DE UBICACION-ADECUACION-ACESSO – SEGURIDAD

1. ¿Actualmente la empresa con la división de Área de Sistemas?

   SI [X] NO [ ]

   OBSERVACIONES:

   (Si la respuesta es NO pase a la pregunta 6)

2. ¿Las instalaciones son las adecuadas, para poder realizar todas las labores en el área de sistemas?

   SI [X] NO [ ]

   OBSERVACIONES

3. ¿Para acceder al área de Sistemas se necesita alguna autorización?

   SI [ ] NO [X]

   OBSERVACIONES:

4. ¿El área de sistemas cuenta con personal de seguridad que restrinja y controle el acceso a las instalaciones de la empresa?

   SI [ ] NO [X]

   OBSERVACIONES:

5. ¿Se hacen revisiones de los equipos periódica y sorpresivamente del contenido de los discos para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa?

   SI [ ] NO [X]

   OBSERVACIONES:

6. ¿La empresa se apega en su totalidad a la estandarización de los Sistemas Operativos, Software utilizado, manejadores de base de datos y se mantienen actualizadas las versiones y la capacitación al personal sobre las modificaciones incluidas?

   SI [ ] NO [X]

   OBSERVACIONES:

7. ¿Existe una salida de emergencia dentro de la empresa?

   SI [X] NO [ ]

   OBSERVACIONES:

8. ¿Los cables de Red, Switch, Routers están de forma adecuada ubicados dentro de la empresa?

   SI [ ] NO [X]

   OBSERVACIONES:

9. ¿Hay comodidad de acuerdo a las distribuciones que se tienen con el equipo de oficina dentro de la empresa?

   SI [X] NO [ ]

   OBSERVACIONES:

10. ¿Existen comprobantes de la adquisición del equipo de cómputo y recursos tecnológicos?

    SI [X] NO [ ]

    OBSERVACIONES:

Apéndice B: Evidencias

Ilustración 15. Revisión de Activos de la empresa FQ Tecnologías

Ilustración 16. Verificación de Activos

Ilustración 17. Entrevista Aux. Contable FQ Tecnologías

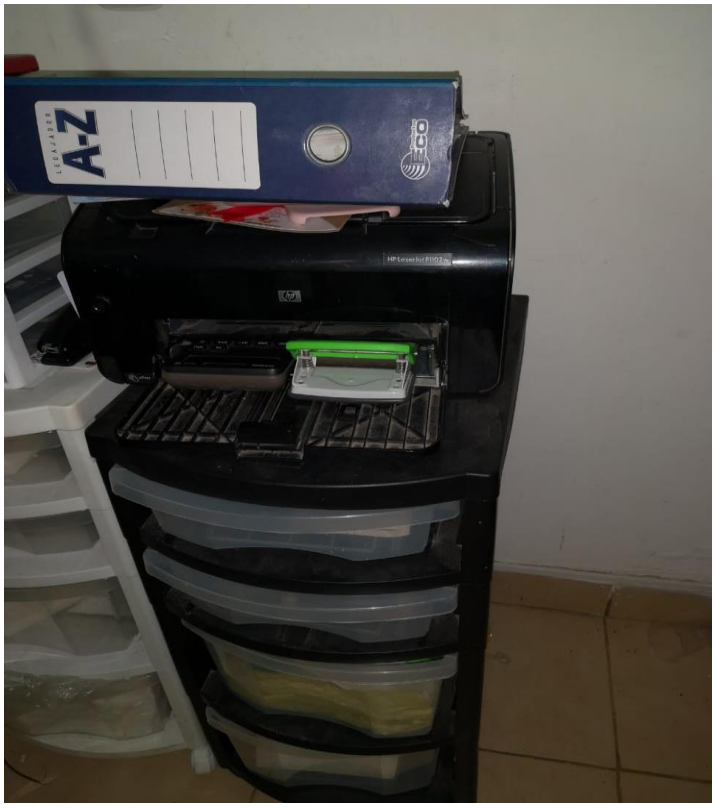


Ilustración 18. Ubicación de Libros Contables y/o otros.

Ilustración 19. Ubicación de Modem Wifi FQ Tecnologías