## RESUMEN - TESIS DE GRADO

| | |
|---|---|
| AUTORES | **LISETH TATIANA ANGARITA LÓPEZ**<br>**MARIA LILIANA SUAREZ DOMINGUEZ**<br>**HULBER RODRIGO RODRIGUEZ PINZÓN** |
| FACULTAD | **DE INGENIERIAS** |
| PLAN DE ESTUDIOS | **ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS** |
| DIRECTOR | **ANDRES MAURICIO PUENTES VELASQUEZ** |
| TÍTULO DE LA TESIS | **DISEÑO DEL PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA CONTROLAR EL ACCESO A LAS AREAS RESTRINGIDAS DE LA EMPRESA INGEPEC LTDA EN LA CIUDAD DE OCAÑA** |


**RESUMEN**
**(70 palabras aproximadamente)**

LA INFORMACIÓN Y LOS PROCESOS, SISTEMAS Y REDES DE APOYO SON ACTIVOS COMERCIALES IMPORTANTES. DEFINIR, LOGRAR Y MEJORAR LA SEGURIDAD DE LA INFORMACIÓN PUEDE SER ESENCIAL PARA MANTENER UNA VENTAJA COMPETITIVA, EL FLUJO DE CAJA, RENTABILIDAD, OBSERVANCIA LEGAL E IMAGEN COMERCIAL.

LAS ORGANIZACIONES Y SUS SISTEMAS Y REDES DE INFORMACIÓN ENFRENTAN AMENAZAS DE SEGURIDAD DE UN AMPLIO RANGO DE FUENTES; INCLUYENDO FRAUDE POR COMPUTADORA, ESPIONAJE, SABOTAJE, VANDALISMO, FUEGO O INUNDACIÓN.


**CARACTERÍSTICAS**

| | | | |
|---|---|---|---|
| PÁGINAS: 90 | PLANOS: | ILUSTRACIONES: 12 | CD-ROM: 1 |

# DISEÑO DEL PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA CONTROLAR EL ACCESO A LAS AREAS RESTRINGIDAS DE LA EMPRESA INGEPEC LTDA EN LA CIUDAD DE OCAÑA

**LISETH TATIANA ANGARITA LÓPEZ**
**MARIA LILIANA SUAREZ DOMINGUEZ**
**HULBER RODRIGO RODRIGUEZ PINZÓN**

**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA**
**FACULTAD DE INGENIERÍAS**
**ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS**
**OCAÑA**
**2014**

# DISEÑO DEL PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA CONTROLAR EL ACCESO A LAS AREAS RESTRINGIDAS DE LA EMPRESA INGEPEC LTDA EN LA CIUDAD DE OCAÑA

**LISETH TATIANA ANGARITA LÓPEZ**
**ARIA LILIANA SUAREZ DOMINGUEZ**
**HULBER RODRIGO RODRIGUEZ PINZÓN**

**Informe final presentado para optar el título de Especialista en Auditoría de Sistemas**

**Director**
**ANDRES MAURICIO PUENTES VELASQUEZ**
**IS. ESP. MSC. Ingeniería de Sistemas y Computación**

**UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA**
**FACULTAD DE INGENIERÍAS**
**ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS**
**OCAÑA**
**2014**

**CONTENIDO**

## LISTA DE CUADROS

Pág.

## LISTA DE TABLAS

Pág.

## LISTA DE GRAFICAS

Pág.

## LISTA DE FIGURAS

Pág.

## LISTA DE ANEXOS

Pág.

# INTRODUCCION

La información y los procesos, sistemas y redes de apoyo son activos comerciales importantes. Definir, lograr y mejorar la seguridad de la información puede ser esencial para mantener una ventaja competitiva, el flujo de caja, rentabilidad, observancia legal e imagen comercial.

Las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas; es por esto que la seguridad de la información es importante en toda organización ya que protege las infraestructuras críticas y funciona como un facilitador para evitar o reducir los riesgos relevantes.

Por lo tanto, en el presente trabajo se diseñó el Plan de Gestión de Seguridad de la Información para controlar el acceso a las áreas restringidas de la empresa INGEPEC LTDA en la ciudad de Ocaña, teniendo en cuenta la necesidad de la organización en establecer las directrices para afrontar riesgos de seguridad de la información que conllevan a que se presenten eventos negativos como la perdida de activos o daño en equipos afectando la calidad del servicio, lo que de manera directa repercute en la perdida de usuarios debido a la carencia de controles eficientes. Siendo este el motivo por el cual se plantea el documento a través de políticas de seguridad con el fin de prevenir algún tipo de ataque que se efectué en contra del activo a proteger y en caso que exista presencia de amenazas se logre tener registro de los sucesos para lograr identificar los responsables y lograr tomar los correctivos e implementar mejores controles.

Con el desarrollo de los objetivos planteados se logra identificar mediante el diagnóstico las falencias que tiene la empresa con relación a la seguridad de la información y definir la estructura y elaboración del Plan de Gestión de Seguridad basado en las Normas ISO/IEC 27001 “Requisitos para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI)” y en la ISO/IEC 27002 “Código de buenas prácticas para la gestión de Seguridad de la información”, obteniendo un documento formal con una serie de lineamentos que permiten controlar el acceso físico a las áreas restringidas de la empresa INGEPEC LTDA .

# 1. DISEÑO DEL PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA CONTROLAR EL ACCESO A LAS AREAS RESTRINGIDAS DE LA EMPRESA INGEPEC LTDA EN LA CIUDAD DE OCAÑA.

## 1.1 PLANTEAMIENTO DEL PROBLEMA

En Colombia las empresas comerciales, industriales, de producción y de servicios han implementado nuevas tecnologías que les han permitido acceder a estrategias que faciliten y hagan más viable la protección de los activos tanto físicos como intangibles, cabe mencionar que cuando se habla de seguridad es importante tener en cuenta que a través de la historia se ha demostrado que esta es importante a nivel externo como interno, de la misma manera que los fracasos más grandes que han tenido grandes compañías han sido proporcionados por personal de la empresa o personas que tienen relación permanente por cualquier otro vinculo, como proveedores o clientes. El país mediante medidas fijadas por entidades del estado permanece en una búsqueda constante de la mejora empresarial y con ello ha logrado concientizar a los grandes empresarios para proteger sus organizaciones y minimizar los riesgos que al no tener los controles necesarios estipulados puede llegar a afectar el correcto desarrollo de las funciones de la entidad, afectando la economía nacional.

A nivel local se puede observar que los administradores de muchas de las empresas son los mismos dueños y por este motivo no se fijan panes de gestión de seguridad adecuadas para resguardar los activos de las mismas, por otra parte al existir vínculos de amistad con los empleados permite que se den atribuciones que no son sanas y vuelven vulnerable la compañía, todo esto surge en la medida que no está estipulada la guía a seguir para que la empresa esté orientada al cumplimiento de la misma

INGEPEC LTDA es una empresa que además de activos valiosos, maneja gran cantidad de información y partiendo del punto de vista que ésta es vulnerable y que las organizaciones deben poseer controles que le permitan protegerla y minimizar los riesgos, INGEPEC LTDA carece del plan de gestión de seguridad que le permita establecer las directrices para afrontar riesgos de seguridad lo cual lleva a que se den eventos negativos para la empresa como la perdida de activos o daño en equipos; afectando la calidad del servicio lo que de manera directa repercute en la perdida de usuarios; de la misma manera es importante mencionar que al no contar con el plan de gestión de seguridad definida que determine aspectos tan importantes como el control de acceso implica que los empleados puedan realizar manipulación de la información y no se cuente con evidencia de las configuraciones que se hagan, además el personal se siente con atribuciones para ingresar a todas las áreas de la empresa, sin importar las consecuencias de los movimientos que se hagan.

## 1.2 FORMULACION DEL PROBLEMA

¿El diseño del plan de gestión de seguridad de la información contribuirá al control de acceso a las áreas restringidas de la empresa INGEPEC LTDA?

## 1.3 OBJETIVOS

**1.3.1General** Diseñar el plan de gestión de seguridad de la información para controlar el acceso a las áreas restringidas de la empresa INGEPEC LTDA.

**1.3.2 Específicos** Realizar un diagnóstico del estado de la seguridad física y de la información de la empresa INGEPEC LTDA.

Identificar y analizar los componentes que integran el Plan de Gestión de Seguridad de la Información para la empresa INGEPEC LTDA de acuerdo a las Normas ISO/IEC 27001 y 27002.

Elaborar el plan de gestión de seguridad de la información mediante una serie de lineamientos que permita controlar el acceso a las áreas restringidas a la empresa INGEPEC LTDA.

## 1.4 JUSTIFICACION

El establecimiento, seguimiento, mejora continua y aplicación de un plan de gestión de seguridad determinado para una empresa establece el compromiso de resguardar los activos y la información de la misma, de igual forma es una muestra de buena administración y organización empresarial debido a que la mayoría de las empresas reconocen la función fundamental que la seguridad desempeña en sus objetivos de negocio, sin embargo no detallan que las infraestructuras de seguridad que hoy en día existen exigen un tiempo de reacción más breve, puesto que los ataques se efectúan con mayor frecuencia. Las organizaciones en ocasiones no pueden reaccionar ante las nuevas amenazas de seguridad antes de que afecten a su negocio, por lo tanto la administración de la seguridad de sus infraestructuras, y el valor de negocio que ofrecen, se ha convertido en una preocupación primordial; por tal razón el tener el plan de gestión de seguridad definido ayuda de manera significativa a la organización para indicar las pautas y de esta manera hacer cumplir los requerimientos para minimizar los riesgos, esta es la medida para contrarrestar los ataques a que las entidades son expuestas actualmente.

Una característica del plan de gestión de seguridad es prevenir algún tipo de ataque que se efectué en contra del activo a proteger y en caso que exista presencia de amenazas se logre tener registro de los sucesos para lograr identificar los responsables y lograr tomar los correctivos e implementar mejores controles.

Cuando la organización no tiene diseñado del plan de gestión de seguridad, no sabe cómo debe actuar y por tanto se está en constante riesgo y se es más vulnerable, cuando éste se fija se está dando el manual preventivo, lo demás dependerá de su correcta aplicación.

## 1.5 HIPOTESIS

Dando respuesta al problema planteado se propone diseñar del plan de gestión de seguridad que integre las condiciones necesarias para el correcto funcionamiento de la empresa INGEPEC LTDA, basada en las normas vigentes en Colombia y que además incluya la sugerencia de implementación de un sistema de identificación biométrico apropiado a los requerimientos de la organización que le facilite administrar el control de acceso a las áreas restringidas.

## 1.6 DELIMITACIONES

**1.6.1 Geográfica** Este estudio tendrá lugar en la empresa INGEPEC LTDA .,en la ciudad de Ocaña Norte de Santander.

**1.6.2 Conceptual** Para la realización de este proyecto se tendrá en cuenta los siguientes conceptos fundamentales como lo son: plan de gestión, seguridad física, control de acceso, sistemas biométricos, seguridad de la información, vulnerabilidad, riesgo, control, administración, sistemas de identificación; haciendo que todos estos términos jueguen un papel importante en el desarrollo del proyecto.

**1.6.3 Temporal** La duración de este proyecto será de 8 semanas, pero si es necesario se ajustara con la aprobación del Director y el comité curricular del plan de estudios.

**1.6.4 Operativa** Si durante el desarrollo del proyecto se presenta alguna dificultad en el alcance de la información, se tendrá en cuenta otras fuentes relacionadas con el tema en estudio, para garantizar la efectividad de los objetivos propuestos.

# 2. MARCO REFERENCIAL

## 2.1 MARCO HISTORICO

La historia de la seguridad inició con una materia prima para su existencia: un riesgo, un peligro, una amenaza. En este sentido, el escenario de la seguridad física se desarrolló en el contexto de la guerra contra un enemigo, que no buscó otra cosa que vulnerar las estrategias de control y contención, entre otras, que tiene el objetivo atacado, para apoderarse de éste.

En la actualidad, la información es el principal activo de muchas organizaciones por lo que es necesario protegerla adecuadamente frente a amenazas que puedan poner en peligro la continuidad del negocio; teniendo en cuenta que la mayor parte de la información reside en equipos informáticos, soportes de almacenamiento y redes de datos, encuadrados dentro de lo que se conoce como sistemas de información; es inevitable que los mismos estén sujetos a riesgos e inseguridades internos y externos a la organización.

Los siguientes trabajos hacen referencia a los aportes que cada autor realizó con respecto a la seguridad de la información y que son fuente para el proyecto:

**SISTESEG[1],** Es una empresa Colombiana líder en servicios de seguridad de la información (SGSI), planes para la continuidad del negocio y Auditorías sobre la infraestructura de tecnología. Cuentan con un equipo humano profesional, comprometido y de amplia experiencia, capaz de interpretar los requerimientos de cualquier empresa y convertirlos en servicios de seguridad de la información hechos a su medida. Su personal cuenta con estudios universitarios de especialización y maestría, en redes y comunicaciones, certificaciones de las compañías multinacionales e institutos certificadores más reconocidos del área de redes y comunicaciones de datos y Seguridad de la Información: CISSP del ISC, CISA de ISACA, ABCP del DRI y COBIT. Esta empresa diseñó sus propias políticas de seguridad física[2] donde identifica las amenazas, vulnerabilidades y las medidas que pueden ser utilizadas para proteger físicamente los recursos y la información de la organización. Los recursos incluyen el personal, el sitio donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan, en general los activos asociados al mantenimiento y procesamiento de la información, como por ejemplo activos de información, activos de software y activos físicos.

**Ciro Antonio Dussan Clavijo,** escribió en el 2006 un artículo sobre "Políticas de seguridad informática" tomando como base la globalización de la economía que ha exigido que las empresas implementen plataformas tecnológicas que soporten la nueva forma de hacer negocios. El uso de Internet para este fin, conlleva a que se desarrollen proyectos de

[1]SISTESEG. [En línea Disponible desde Internet en: < http://www.sisteseg.com/>[con acceso el 8-12-2013]
[2]POLITICA DE SEGURIDAD FÍSICA. SISTESEG. [En línea]. Disponible desde Internet en: <http://www.sisteseg.com/files/Microsoft_Word_-_Politica_Seguridad_Fisica.pdf>[con acceso el 06-03-2013]

seguridad informática que garanticen la integridad, disponibilidad y accesibilidad de la información. La creación de políticas de seguridad es una labor fundamental que involucra las personas, los procesos y los recursos de la compañía. Este artículo presenta los puntos clave a tener en cuenta para diseñar una política de seguridad basándose en la norma ISO 17799.[3]

**Arean Hernando Velasco Melo[4],** escribió en el 2008 un artículo sobre "el derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27001". Este artículo pretende informar sobre la existencia y diversas modalidades que incluye el Derecho informático y crear conciencia acerca de la posición que deben tomar los diversos actores económicos en la era de la información para asegurar una adecuada política de seguridad de la información que, ante la falta de una legislación nacional sobre el tema, debe basarse en los estándares internacionales, el derecho comparado y autonomía de la voluntad. La metodología empleada para explicar las diversas áreas de impacto es la seguida por la norma ISO 27001 en el dominio que hace referencia al cumplimiento y que comprende: La protección de datos personales; la contratación de bienes informáticos y telemáticos; el derecho laboral y prestación de servicios, respecto de la regulación de aspectos tecnológicos; los servicios de comercio electrónico; la propiedad intelectual, y el tratamiento de los incidentes informáticos.

**Comité de Seguridad de la Información de la Universidad Tecnológica Nacional de Argentina**[5], en el año 2009 ha elaborado y coordinado un plan para crear e implementar sus propias políticas de seguridad de la información, basándose en las características establecidas en el Modelo de Política de Seguridad de la Información para Organismos de la Administración Pública Nacional, publicado por la Oficina Nacional de Tecnología de Información ONTI.

## 2.2 MARCO TEORICO

**2.2.1 Teoría General de la Información**, Ángel Benito, Profesor del departamento de periodismo III de la Universidad Complutense de Madrid, describe que:

[3]DUSSAN CLAVIJO, Ciro Antonio; 2006 (Enero - Junio). Políticas de seguridad informática. Vol.2 No. 1 [En línea]. Disponible desde Internet en: <http://www.unilibrecali.edu.co/entramado/images/stories/pdf_articulos/volumen2/Politicas_de_seguridad_informtica.pdf>[con acceso el 06-03-2013]

[4]VELASCO MELO, Arean Hernando; Junio 2008 Rev. Derecho no.29 Barranquilla. El derecho informático y la gestión de la seguridad de la información una perspectiva con base en la norma ISO 27001. [En línea]. Disponible desde Internet en:<http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-86972008000100013>[con acceso el 06-03-2013]

[5]COMITÉ DE SEGURIDAD DE LA INFORMACIÓN DELA UNIVERSIDAD TECNOLÓGICA NACIONAL DE ARGENTINA. Políticas de seguridad de la información. [En línea]. Disponible desde Internet en: <http://www.utn.edu.ar/comiteseguridad/documentoscsi.utn>[con acceso el 01-03-2013]

"La Teoría General de la Información[6] es la disciplina más amplia de cuantas se ocupan del hecho social de la información y comunicación colectivas. Es una ciencia nueva, básica, imprescindible para una comprensión acabada del fenó-meno contemporáneo que hemos convenido en llamar comunicaciones de masas... Denominé esta disciplina como Teoría General de la Información en 1960, tras de explicar durante varios cursos una Introducción al Periodismo y después de valorar las experiencias académicas que en Europa y en América... se venían haciendo a raíz de la Segunda Guerra Mundial".

En esta descripción del proceso informativo hay diez elementos y de ellos se deducen las distintas especialidades científicas que se ocupan de la información, que serán disciplinas particulares en contraposición con las generales dedicadas a estudiar, desde diversas posiciones científicas.

Pormenorizando, aunque sin agotarlos, los diez elementos del proceso son.

**Quién.** Es la Fuente; si en el proceso informativo puede otorgarse alguna vez alguna prioridad a uno de sus elementos, es éste; este primer quién puede desatar activamente todo el proceso; de algún modo, así lo hace, cuando, por ejemplo, un periodista descubre un hecho noticioso y lo da a conocer.

**Qué.** Es el contenido que se informa, que circula por los canales informativos, y que al ser compartido por un público se constituye en objeto de la comunicación.

Canal es el medio utilizado para trasladar 1 mensaje; puede ser un medio mecánico para una simple transmisión, como el teléfono, o un instrumento complicado para la difusión a un público amplio, como la prensa, la radio, el cine, etc.

**Cómo.** Expresa tanto la forma que recibe el mensaje para adecuarse al canal y al público como el tratamiento organizativo que requieren los distintos contenidos para ser informados y comunicados.

**A quién.** Para entendernos, diremos que es el término que recibe la información, el que se beneficia del contenido informativo; en los instrumentos masivos de comunicación, este quién debe ser asimilado al público.

**Qué consecuencias.** Sin más precisión aquí, las secuelas de todo tipo que en el quién receptor del mensaje produce éste.

**Por qué.** Es una circunstancia que corresponde al primer quién; qué se propone, cuáles son sus propósitos, qué busca tal empresa informativa cuando se constituye en fuente de noticias, por ejemplo.

[6]LA TEORÍA GENERAL DE LA INFORMACIÓN, UNA CIENCIA MATRIZ. [En línea]. Disponible desde Internet en: <http://www.infoamerica.org/teoria_articulos/benito01.pdf>[con acceso el 07-03-2013]

**Bajo qué condiciones y responsabilidad**. ¿en qué circunstancias opera el quién fuente? ¿Con qué estatuto jurídico? ¿Con qué medios técnicos?

**Qué medios auxiliares**. Al considerar, por ejemplo, la prensa, la publicidad es para ella un medio auxiliar, una contribución legítima que le permite una más amplia difusión. Y al revés, si consideramos la publicidad, ésta que en sí misma es una actividad informativa más, para la realización de sus fines, utiliza como auxiliar a la prensa y a los otros instrumentos informativos.

**Qué circunstancia social.** Pues, bien, el objeto propio de la Teoría General de la Información no es otro que el estudio del conjunto de elementos acabados de enumerar. La IGl estudia los elementos humanos del proceso, los elementos técnicos y organizativos, el contenido y la forma de las informaciones y de manera muy especial, las relaciones dinámicas que se establecen ente todos estos elementos.

El carácter de ciencia matriz de la Teoría General de la Información la sitúa como precedente académico necesario para el desglose pormenorizado de las disciplinas particulares destinadas al estudio e investigación de cada uno de los diez elementos del proceso comunicativo, que, en conjunto, son su objeto propio de estudio. Es un precedente necesario, de carácter general, tanto para este desarrollo de las disciplinas especializadas, como para la preparación académica de los futuros profesionales.

**2.2.2 Teoría del Sistema.** La teoría de la organización y la práctica administrativa han experimentado cambios sustanciales en años recientes. La información proporcionada por las ciencias de la administración y la conducta ha enriquecido a la teoría tradicional. Estos esfuerzos de investigación y de conceptualización a veces han llevado a descubrimientos divergentes. Sin embargo, surgió un enfoque que puede servir como base para lograrla convergencia, el enfoque de sistemas, que facilita la unificación de muchos campos del conocimiento. Dicho enfoque ha sido usado por las ciencias físicas, biológicas y sociales, como marco de referencia para la integración de la teoría organizacional moderna.

El primer expositor de la Teoría General de los Sistemas fue Ludwig von Bertalanffy, en el intento de lograr una metodología integradora para el tratamiento de problemas científicos.

La meta de la Teoría General de los Sistemas no es buscar analogías entre las ciencias, sino tratar de evitar la superficialidad científica que ha estancado a las ciencias. Para ello emplea como instrumento, modelos utilizables y transferibles entre varios continentes científicos,toda vez que dicha extrapolación sea posible e integrable a las respectivas disciplinas[7]

[7]Ibid. p. 50

## 2.3 MARCO CONCEPTUAL

El proyecto incluye el concepto de seguridad física el cual se define según la Norma NS/03 como la condición que se alcanza en las instalaciones cuando se aplica un conjunto de medidas de protección eficaces para la prevención de posibles accesos a información clasificada por parte de personas no autorizadas, así como para proporcionar las evidencias necesarias cuando se produzca un acceso o un intento de acceso[8].

Según la Norma ISO 27002 las áreas de trabajo de la organización y sus activos deben ser clasificadas y protegidas en función de su criticidad, siempre de una forma adecuada y frente a cualquier riesgo factible de índole física (robo, inundación, incendio...).

El término seguridad de la información se define en la Norma como la preservación de confidencialidad, integridad y disponibilidad de la información; además también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudiación y confiabilidad; donde a su vez se define la confidencialidad como el aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso, la integridad es la garantía de la exactitud y completitud de la información y de los métodos de su procesamiento y la disponibilidad es el aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados[9].

**2.3.1 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 comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

**2.3.2 Activo.**Cualquier cosa que tenga valor para la organización

**2.3.3 Control.**Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

**2.3.4 Vulnerabilidad.**La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas.

**2.3.5 Riesgo.**Combinación de la probabilidad de un evento y su ocurrencia.

**2.3.6 Tratamiento del riesgo.**Proceso de selección e implementación de medidas para modificar el riesgo

[8]CENTRO NACIONAL DE INTELIGENCIA, Autoridad Nacional para la protección de la información clasificada, Norma NS/03, Edición 2.0 Diciembre 2012

[9] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. Bogotá D.C.: ICONTEC, 2007. NTC ISO/IEC 27002

**2.3.7 Amenaza.**Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.

**2.3.8 Control de acceso.** Es la habilidad de permitir o denegar el uso de un recurso particular a una entidad en particular.

Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos (ej. acceso a una habitación donde hay servidores), recursos lógicos (ej. una cuenta de banco, de donde solo determinadas personas pueden extraer dinero) o recursos digitales (ej. un archivo informático que sólo puede ser leído, pero no modificado)

**2.3.9 Sistemas biométricos.** Se utilizan para la identificación automática de personas mediante el uso de características físicas del individuo o de su comportamiento. Estas pueden ser su cara, el iris de los ojos o sus huellas dactilares. Son rasgos únicos e intransferibles de cada persona.

## 2.4 MARCO LEGAL

**2.4.1 Constitución Política de Colombia**. Artículo 61[10]. El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley.

**2.4.2 Norma ISO/IEC27002**. Tecnología de la información, técnicas de seguridad[11]. Código para la práctica de la gestión de la seguridad de la información. Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

Esta norma puede servir como guía práctica para el desarrollo de normas de seguridad de la organización y para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones.

**2.4.3 Ley 1273 de 2009 (5 de enero)**. El Congreso de la República de Colombia, establece la ley 1273[12] por medio de la cual se modifica el Código Penal, creando un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

El proyecto tendrá como bases legales la ley 1273 de 2009, en sus artículos:

**Artículo 269A: Acceso abusivo a un sistema informático.** El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con

[10]REPÚBLICA DE COLOMBIA, Constitución Política De La República De Colombia De 1991,Actualizada hasta el Decreto 2576 del 27 de Julio de 2005
[11]ISO, Op. cit.
[12]CONGRESO DE LA REPUBLICA COLOMBIANA. Op. cit.

una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

**Artículo 269B. Obstaculización ilegítima de sistema informático o red de telecomunicación.** El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

**Artículo 269C. Interceptación de datos informáticos.** El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

**Artículo 269D. Daño Informático.** El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

# 3. DISEÑO METODOLOGICO

## 3.1 TIPO DE INVESTIGACION

En el desarrollo del proyecto se utilizó el método basado en una investigación descriptiva con enfoque cuantitativo el cual, como lo manifiesta BERNAL TORRES, Cesar Augusto en su libro Metodología de la Investigación, citando a SALKING, Neil "se reseñan las características o rasgos de la situación o fenómeno objeto de estudio".

Con la aplicación de éste método se buscó obtener información sobre la situación actual de la empresa INGEPEC LTDA en lo referente a la seguridad física y del entorno.

## 3.2 POBLACION Y MUESTRA

La población objeto de estudio se conformó por diez (10) personas que laboran en la empresa INGEPEC LTDA :

**Cuadro 1.** Relación de empleados que conforman la población objeto de estudio.

| NOMBRE | CARGO |
|---|---|
| Fernando Augusto Pérez | Gerente |
| Said Angarita | Técnico en Mantenimiento |
| Nancy Rodríguez | Administradora |
| Teresa Güillín | Secretaria |
| Yamile de Güillín | Cajera |
| David Martínez | Técnico en Mantenimiento |
| Jorge Huron | Técnico en Mantenimiento |
| Hernán Robles | Técnico en Mantenimiento |
| Ludy Rodríguez | Contadora |
| Mery Gutiérrez | Auxiliar Contable |

**Fuente**. Autores del proyecto

Para el desarrollo del proyecto se hizo necesario trabajar con el cien por ciento (100%) de la población teniendo en cuenta que es finita, por lo que no se requirió la aplicación de fórmulas estadísticas.

## 3.3 TECNICAS DE RECOLECCION DE DATOS

La recolección de la información necesaria para la investigación se realizó mediante las técnicas de la observación, revisión documental, listas de chequeo, encuestas y entrevistas aplicadas al Gerente de la empresa INGEPEC y al personal que allí labora.

## 3.4 ANALISIS DE RESULTADOS

El análisis de la información recopilada a través de los instrumentos se realizó de manera cuantitativa y cualitativa describiendo los resultados obtenidos, basándonos en las Normas ISO/IEC 27001 y 27002.

# 4. ANALISIS Y DISCUSIÓN DE RESULTADOS

## 4.1 DIAGNÓSTICO DE LA SEGURIDAD FÍSICA Y DE LA INFORMACIÓN DE LA EMPRESA INGEPEC LTDA.

En la actualidad los procesos de negocios y la infraestructura tecnológica están expuestos a un importante nivel de amenazas tanto externas como internas; que ponen en riesgo la seguridad de la información y los activos utilizados en el desarrollo de las operaciones de la empresa, es por este motivo que se hace necesario realizar un diagnóstico a la empresa INGEPEC LTDA que permita conocer los riesgos asociados a su entorno y saber cómo se encuentra su nivel de seguridad física y de la información.

El propósito de esta primera fase fue identificar el estado actual de la seguridad de la información y la importancia de implementar un plan de gestión en la empresa de televisión INGEPEC LTDA de la ciudad de Ocaña.

Con el fin de dar cumplimiento al objetivo general del diagnóstico propuesto se realizaron las actividades relacionadas a continuación

**4.1.1 Aplicación de encuesta a los empleados de INGEPEC LTDA.** Con ésta encuesta se pretende rrecolectar información para conocer la necesidad de diseñar el plan de gestión de seguridad para controlar el acceso a las áreas restringidas de la empresa INGEPEC LTDA.

Sus resultados permitirán conocer políticas desarrolladas en dicha empresa para definir el estado en el que se encuentra actualmente.

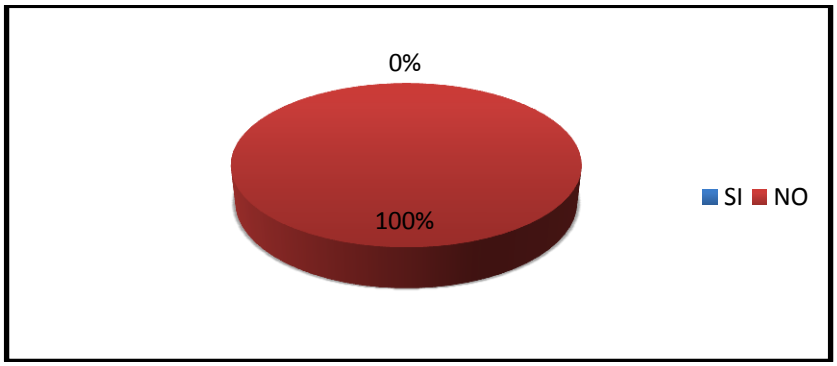
Resultados de la encuesta aplicada

**Tabla 1.** La empresa cuenta con un plan de gestión de seguridad de la información.

| RESPUESTA | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 0 | 0% |
| NO | 10 | 100% |
| Total | 10 | 100% |

**Fuente**. Autores del proyecto

**Gráfico 1.** Cuenta la empresa con un plan de gestión de seguridad de la información




**Fuente**. Autores del proyecto

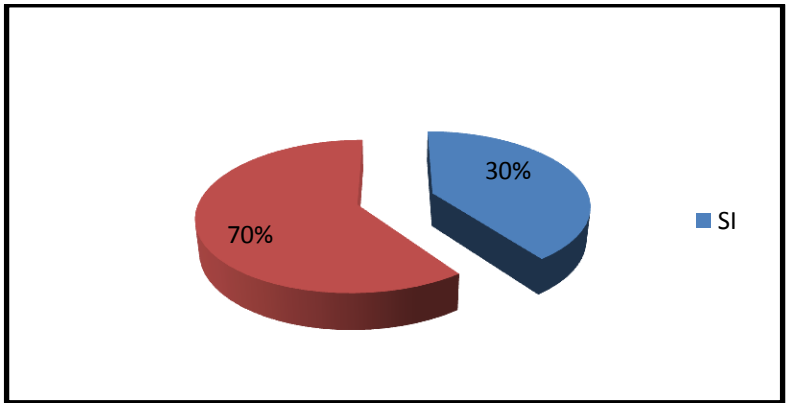
Teniendo en cuenta la respuesta dada por los empleados de INGEPEC LTDA el 100% afirmo que la empresa no cuenta con un plan de gestión de seguridad de la información, lo cual lleva a que se den eventos negativos para ella, como la perdida de activos o daño en equipos; afectando la calidad del servicio que de manera directa repercute en la perdida de usuarios, haciendo que se puedan presentar riesgos como perdida o daño de la información afectando la seguridad de la misma.

**Tabla 2.** Se utiliza perímetros de seguridad para proteger las áreas que contienen información y medios de procesamiento de la misma.

| RESPUESTA | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 3 | 30% |
| NO | 7 | 70% |
| Total | 10 | 100% |

**Fuente**. Autores del proyecto

**Gráfico 2.** Se utiliza perímetros de seguridad para proteger las áreas que contienen información y medios de procesamiento de la misma.




**Fuente**. Autores del proyecto

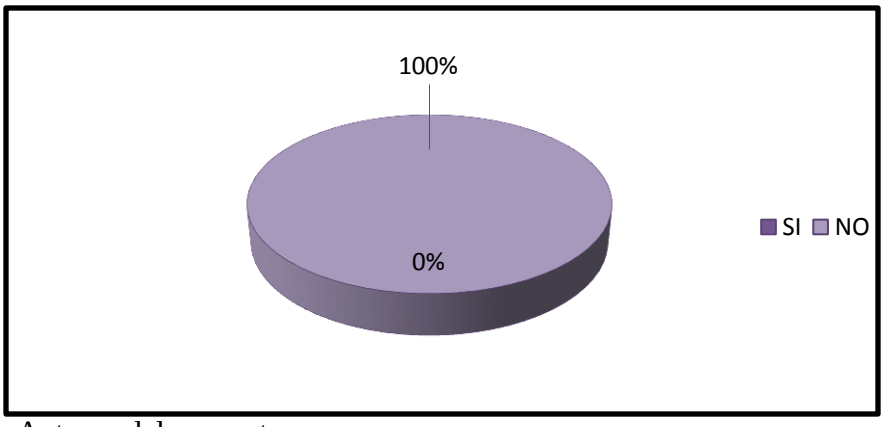
Teniendo en cuenta las respuestas dadas por el personal de INGEPEC LTDA; se puede establecer que el 70% de ellos manifiestan que no existen perímetros de seguridad definidos en la empresa, mientras que el 30% consideran como perímetros de seguridad algunas áreas donde se encuentran almacenados los equipo; lo que indica que debe definirse un perímetro de seguridad protegido del acceso no autorizado, daño e interferencia, de igual manera se debe comunicar al personal sobre la existencia del mismo y realizar la debida señalización;; permitiendo que sea identificado por el total de empleados.

**Tabla 3.** Existen mecanismos para el control de acceso a áreas seguras.

| RESPUESTA | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 10 | 100% |
| NO | 0 | 0% |
| Total | 10 | 100% |

**Fuente**. Autores del proyecto

**Grafico 3.** Existen mecanismos para el control de acceso a áreas seguras.




**Fuente**. Autores del proyecto

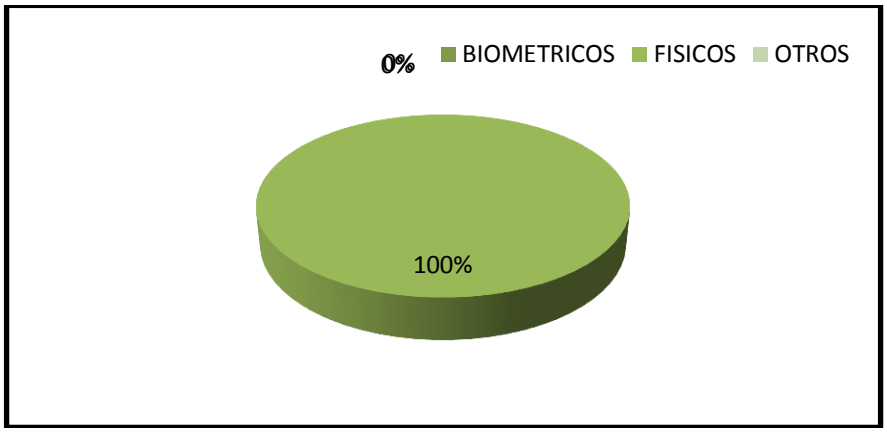
El 100% de los encuestados afirma que si existen mecanismos de control de acceso a áreas seguras, considerando como estos las cerraduras metálicas y candados; lo cual indica que estas herramientas no brindan la seguridad adecuada para garantizar la protección de la información.

**Tabla 4.** Mecanismos para el control de acceso utilizados en INGEPEC LTDA

| RESPUESTA | FRECUENCIA | PORCENTAJE |
|---|---|---|
| BIOMETRICOS | 0 | 0% |
| FISICOS | 10 | 100% |
| OTROS | 0 | 0% |
| Total | 10 | 100% |

**Fuente**. Autores del proyecto

**Gráfico 4.** Mecanismos para el control de acceso utilizados en INGEPEC LTDA




**Fuente**. Autores del proyecto

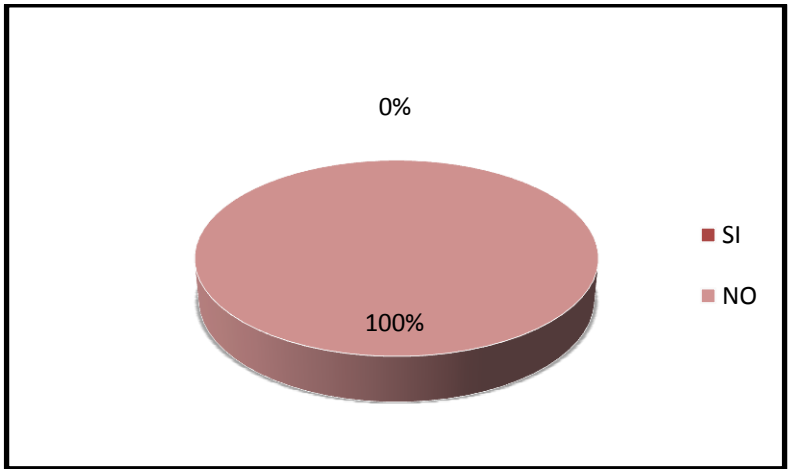
Del total de los encuestados el 100% indico que los mecanismos para el control de acceso utilizados en INGEPEC son físicos, sin embargo estos controles no son los apropiados para asegurar que solo se le permita el acceso al personal autorizado.

**Tabla 5.** Existencia de lineamientos para trabajar en áreas aseguradas

| RESPUESTA | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 0 | 0% |
| NO | 10 | 100% |
| Total | 10 | 100% |

**Fuente**. Autores del proyecto

**Grafico 5.** Existencia de lineamientos para trabajar en áreas aseguradas




**Fuente**. Autores del proyecto

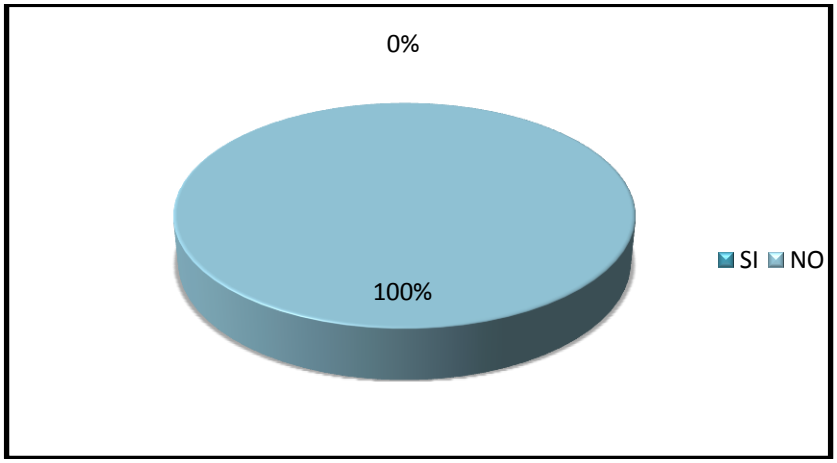
El 100% del personal encuestado afirma que no existen lineamientos para trabajar en áreas seguras, lo cual ocasiona que los empleados no estén al tanto de la existencia de actividades dentro del área asegurada ni que la misma pueda ser supervisada para evitar actividades maliciosas que pongan en riesgo la información.

**Tabla 6.** Existencia de métodos de protección de equipos

| RESPUESTA | FRECUENCIA | PORCENTAJE |
|---|---|---|
| SI | 0 | 0% |
| NO | 10 | 100% |
| Total | 10 | 100% |

**Fuente**. Autores del proyecto

**Grafico 6.** Existencia de métodos de protección de equipos




**Fuente**. Autores del proyecto

Teniendo en cuenta la respuesta de los encuestados el 100% del personal indica que no existen mecanismos de protección de equipos, lo cual ocasiona que la información se encuentre expuesta a amenazas y peligros ambientales por no contar con controles que protejan los equipos y reduzcan los riesgos.

Con el ánimo de conocer de manera general la estructura organizacional, las áreas de la empresa INGEPEC LTDA, los procesos principales que desarrolla, los objetivos misionales de la misma y la caracterización de la información que administra.

**4.1.2 Direccionamiento estratégico de INGEPEC LTDA.** La empresa INGEPEC LTDA., nació hace 24 años con el montaje del sistema de parabólica en el Municipio Ocaña, este proyecto fue un éxito puesto que ofrecía una programación variada, para todos los gustos y edades.

INGEPEC LTDA, ofrece a la comunidad el servicio de televisión por suscripción y en la actualidad funciona como una empresa que cuenta con nueve empleados; se ha mantenido en el mercado gracias a la calidad y continuidad en el servicio. Su estructura administrativa, contable y fiscal han permitido que la entidad permanezca fortalecida y funcionando a lo largo del tiempo.

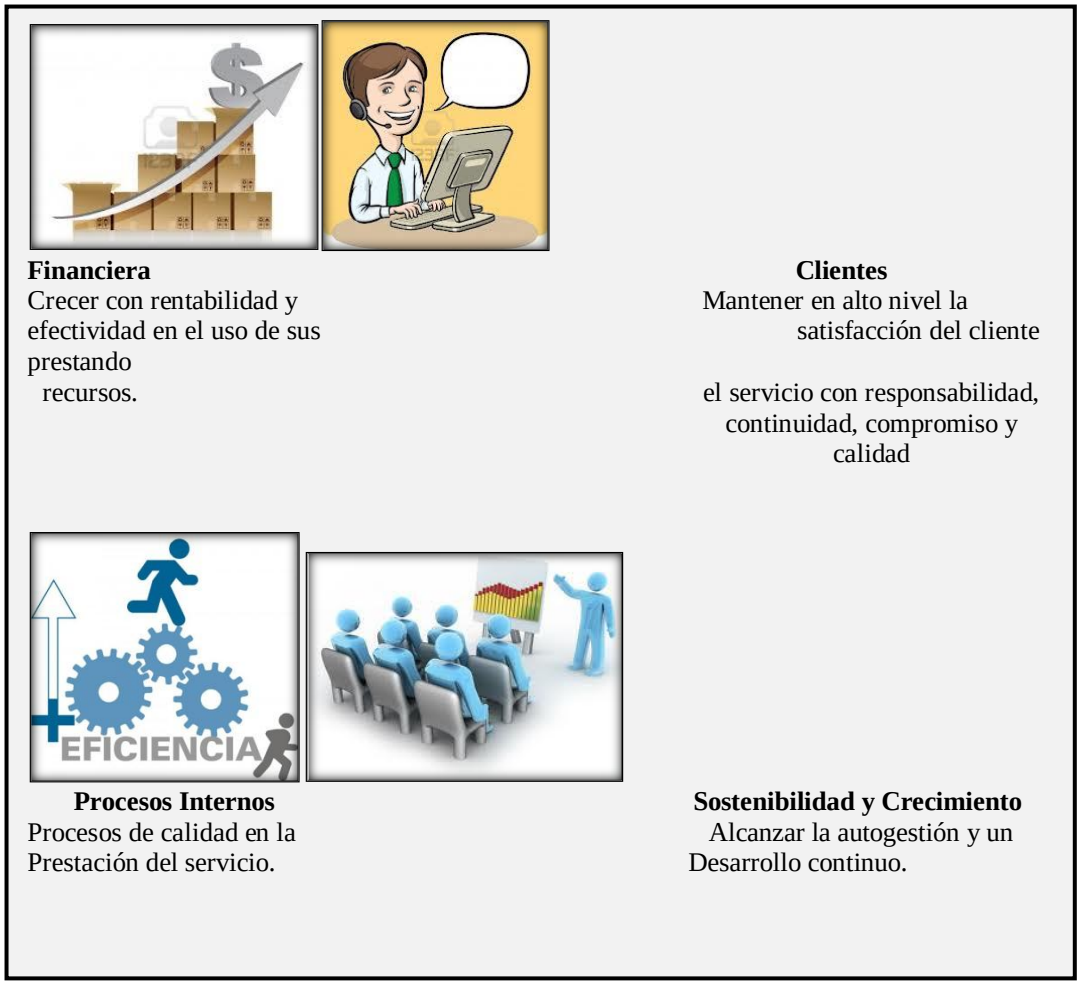
Es una sociedad de responsabilidad Limitada por lo que es primordial que la Dirección y los socios consideren indispensable la seguridad de la información como factor principal que aseguren los activos y por ende la inversión realizada por cada socio, a través de la ejecución de controles efectivos.

**Modelo de Objetivos.** La empresa INGEPEC LTDA ., vincula directamente su objetivo general con la misión y visión de la empresa. (Figura 1.)

**Misión.** INGEPEC LTDA como empresa líder y pionera en la prestación del servicio de televisión por suscripción, ofrece a la ciudad de Ocaña excelentes canales internacionales, nacionales, regionales y de producción propia. Con tecnología y talento humano capacitado en asesorías, montajes e instalaciones, para satisfacer las necesidades de la población afiliada al servicio y así mejorar su calidad de vida utilizando la televisión como un instrumento integrador de la familia; a través de la cultura, educación, información y entretenimiento de nuestros suscriptores y del resto de la comunidad.

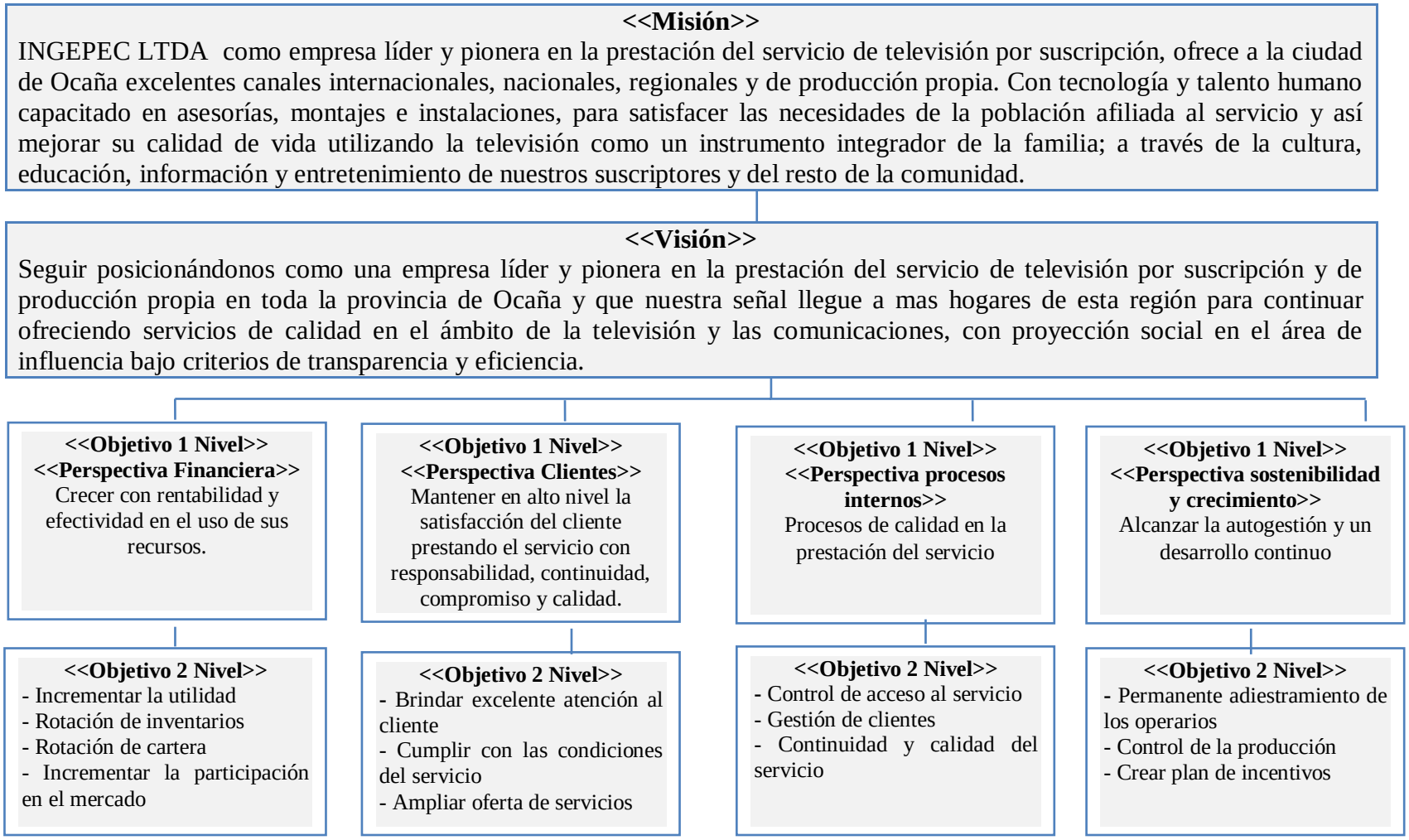
**Visión.** Seguir posicionándonos como una empresa líder y pionera en la prestación del servicio de televisión por suscripción y de producción propia en toda la provincia de Ocaña y que nuestra señal llegue a mas hogares de esta región para continuar ofreciendo servicios de calidad en el ámbito de la televisión y las comunicaciones, con proyección social en el área de influencia bajo criterios de transparencia y eficiencia.

**Figura 1.** Objetivos de la empresa INGEPEC LTDA .




**Fuente**. Autores del proyecto

**Cuadro 2.** Misión, Visión y objetivos de la empresa INGEPEC LTDA .




**Fuente**. Autores del proyecto

Durante el desarrollo del proyecto se evidencia la necesidad que tiene la empresa INGEPEC LTDA., de evaluar la misión y visión a través de una serie de criterios que permitan crear estrategias que contribuyan a la eficiencia, eficacia y efectividad de los procesos de la organización. Es por ello que la seguridad de la información ayuda a la misión de la empresa protegiendo sus recursos físicos y financieros, reputación, posición legal, empleados y otros activos tangibles e intangibles. Por lo anterior se realiza la evaluación planteando una nueva misión y visión que cumpla con las características necesarias que preserven los procesos comerciales de fallas o desastres en los sistemas de información asegurando la reanudación oportuna de las operaciones esenciales garantizando de esta manera la consecución de los objetivos y la continuidad del negocio.

**Cuadro 3.** Evaluación de la Misión

| **Misión actual:** INGEPEC LTDA como empresa líder y pionera en la prestación del servicio de televisión por suscripción, ofrece a la ciudad de Ocaña excelentes canales internacionales, nacionales, regionales y de producción propia. Con tecnología y talento humano capacitado en asesorías, montajes e instalaciones, para satisfacer las necesidades de la población afiliada al servicio y así mejorar su calidad de vida utilizando la televisión como un instrumento integrador de la familia; a través de la cultura, educación, información y entretenimiento de nuestros suscriptores y del resto de la comunidad. | | | | |
|---|---|---|---|---|
| **N°** | **CRITERIOS** | **PREGUNTA** | **SI** | **NO** |
| **1** | Clientes | ¿Quiénes son los clientes? | X | |
| **2** | Productos y servicios | ¿Cuáles son los servicios o productos más importantes? | X | |
| **3** | Mercados | ¿Compite geográficamente? | | X |
| **4** | Tecnología | ¿Cuál es la tecnología básica? | X | |
| **5** | Preocupación por supervivencia, crecimiento y rentabilidad | ¿Cuál es la actitud de la organización en relación a metas económicas? | | X |
| **6** | Filosofía | ¿Cuáles son las creencias básicas, los valores, las aspiraciones, las prioridades éticas de la organización? | X | |
| **7** | Concepto de sí misma | ¿Cuáles son las ventajas competitivas claves? | X | |
| **8** | Preocupación por la imagen pública | ¿Cuál es la imagen pública a que aspira?, ¿Es responsable socialmente, ante la comunidad y el medio ambiente? | | X |
| **9** | Preocupación por los empleados | ¿Son los empleados un valor activo para la organización? ¿Pone atención a los deseos de las personas claves, de los grupos de interés? | X | |

**Fuente**. Autores del proyecto

Realizada la evaluación de la misión se concluye que:

No incluye la competencia de mercado.
No tiene en cuenta la preocupación por supervivencia, crecimiento y rentabilidad.
No refleja la preocupación por la imagen pública.

**Misión Propuesta.** INGEPEC LTDA es una empresa que presta el servicio de televisión por suscripción, ofreciendo a los ciudadanos de Ocaña excelentes canales internacionales, nacionales, regionales y de producción propia con calidad; satisfaciendo las necesidades de la comunidad a través de la transmisión de cultura, entretenimiento e información veraz y oportuna, como instrumento integrador de la familia que propende por el cuidado del medio ambiente y responsabilidad social. Con tecnología de punta y personal idóneo, que le permite competir en el mercado con una rentabilidad económica y crecimiento sostenible.

**Cuadro 4.** Evaluación de la Visión

| **Visión actual:** Seguir posicionándonos como una empresa líder y pionera en la prestación del servicio de televisión por suscripción y de producción propia en toda la provincia de Ocaña y que nuestra señal llegue a mas hogares de esta región para continuar ofreciendo servicios de calidad en el ámbito de la televisión y las comunicaciones, con proyección social en el área de influencia bajo criterios de transparencia y eficiencia. | | | |
|---|---|---|---|
| **N°** | **CRITERIO** | **SI** | **NO** |
| 1 | Orientado al futuro incluso en su redacción | | X |
| 2 | Es integradora | | X |
| 3 | Es corta | X | |
| 4 | Es positiva y alentadora | X | |
| 5 | Es realista - posible | X | |
| 6 | Es consistente con los principios y valores de la organización | | X |
| 7 | Orienta la transición de los que es a lo que debe llegar a ser | | X |
| 8 | Expresa claramente los logros que se esperan en el periodo | | X |
| 9 | Cubre todas las áreas actuales y futuras de la organización | | X |
| 10 | Está redactada en términos que signifiquen acción | | X |
| 11 | Tienen fuerza e impulsa a la acción | | X |
| 12 | Contiene el futuro visualizado | | X |
| 13 | Es el sueño alcanzable a largo plazo | | X |

**Fuente**. Autores del proyecto

Realizada la evaluación de la Visión se concluye que:

No cumple con la mayoría de los ítems de la evaluación, por lo tanto se propone una Visión para la empresa INGEPEC LTDA . orientada al futuro, medible, integradora, redactada en términos de acción y alcanzable a lo largo del tiempo.

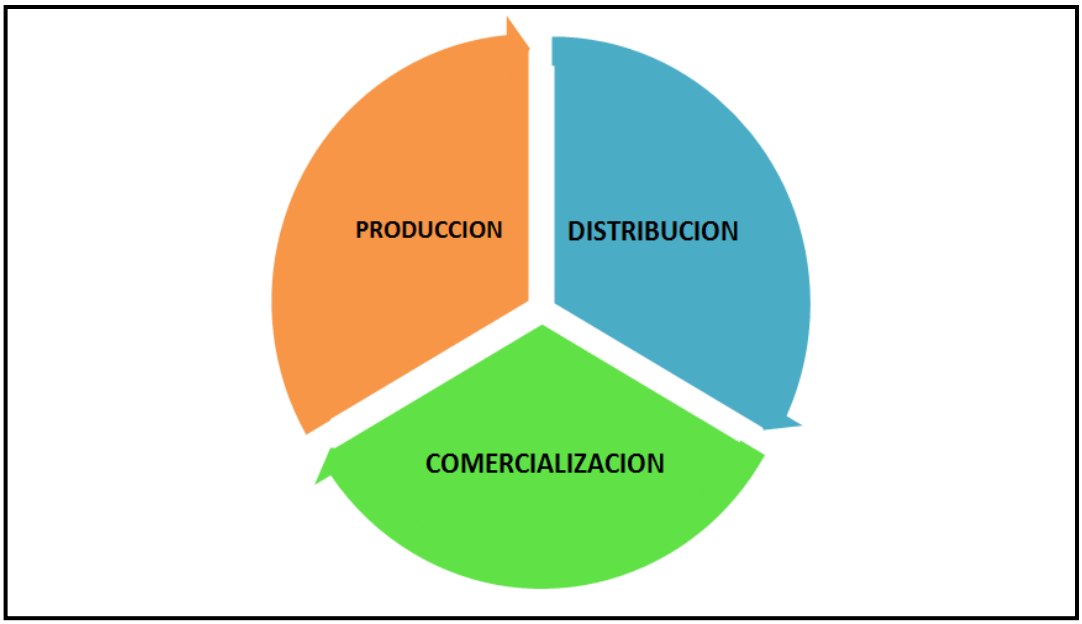
**Visión Propuesta.** INGEPEC LTDA para el 2018 será reconocida como una empresa líder y competitiva por su excelencia y calidad en la prestación del servicio de televisión, a través del uso de las tecnologías de la información y las comunicaciones, aumentando la base de contenidos en diferentes formatos novedosos además de la producción propia de alta calidad bajo un marco de responsabilidad social y ambiental.

**Figura 2.** Estructura Organizacional


**Fuente**. Autores del proyecto

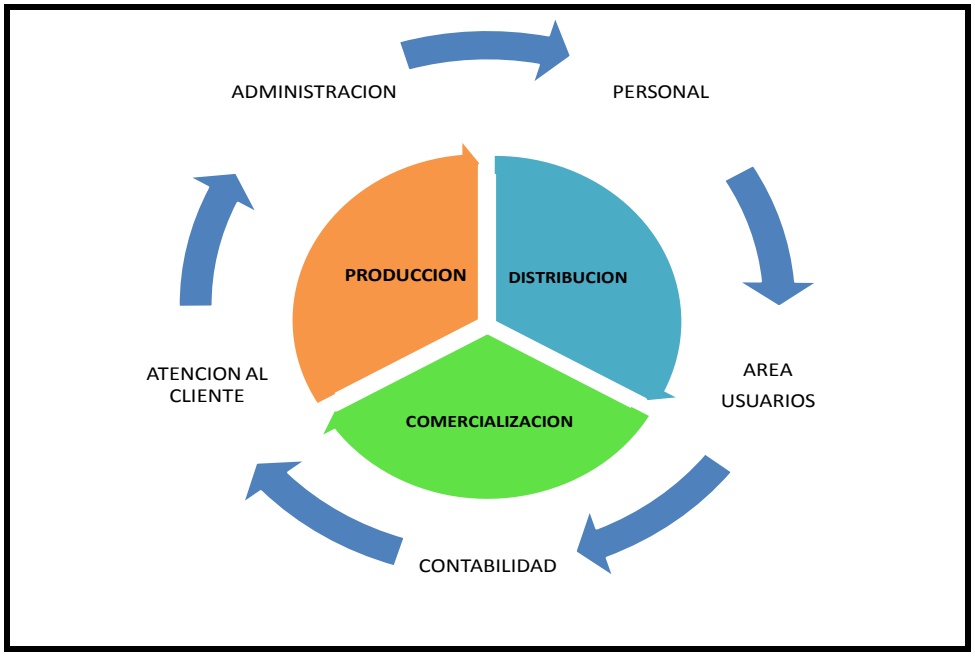
**Procesos de INGEPEC LTDA**

**Figura 3.** Procesos Principales



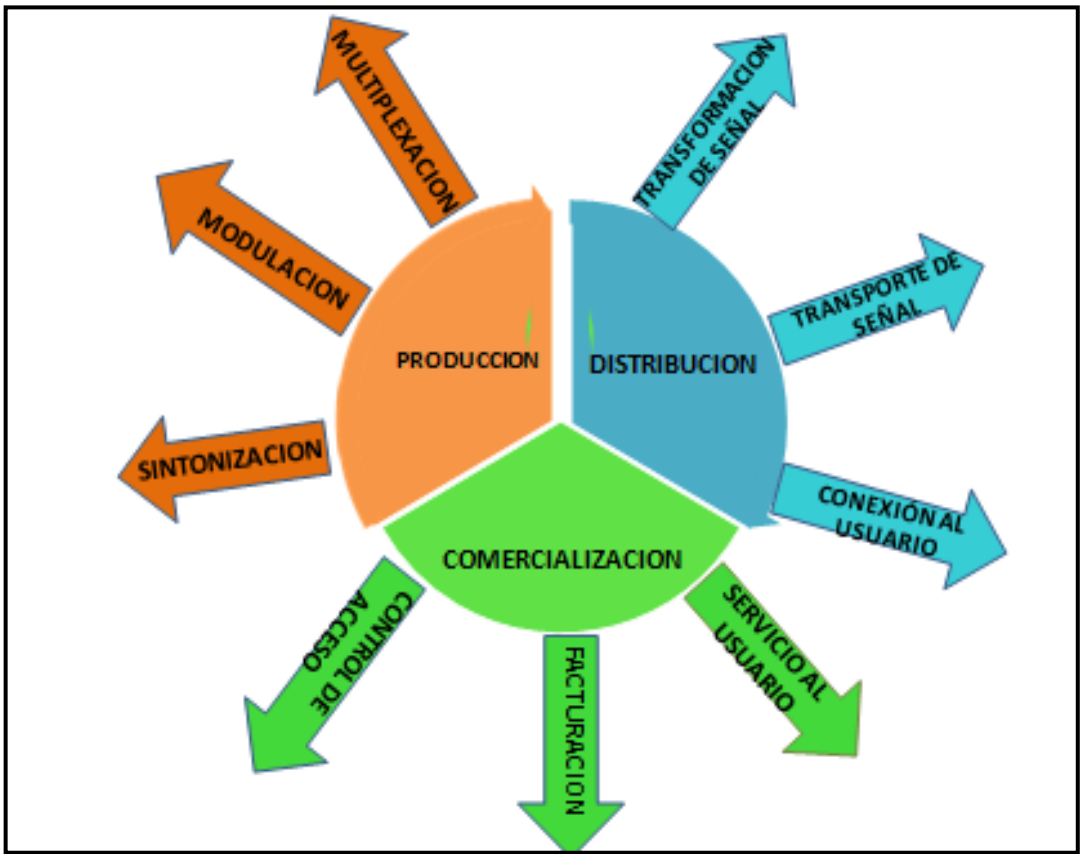

**Fuente**. Autores del proyecto

**Figura 4.** Procesos de apoyo




**Fuente**. Autores del proyecto

**Figura 5.** Procesos principales y sus subprocesos




**Fuente**. Autores del proyecto

**Proceso de producción**

**Subproceso Sintonización.** Armado de antenas, orientación de antenas, Ubicación de satélites y Calibración de sintonizadores LNB.

**Subproceso Modulación.** Procesamiento de señal, Selección de canales disponibles, Configuración de equipos.

**Subproceso Multiplexación.** Combinación de canales en un solo paquete para obtener la señal de salida.

**Proceso de distribución**

**Subproceso Transformación de señal.** Calibrar los amplificadores para distribuir la señal en un nivel adecuado por toda la red, mediante dichos amplificadores la señal experimenta transformaciones en sus niveles con el fin de alcanzar el cubrimiento de largas distancias.

**Subproceso Transporte de señal.** Extender redes principales o troncales, instalación de dispositivos derivadores de señal y amplificadores, ampliar la cobertura del servicio a nuevos usuarios.

**Subproceso Conexión al usuario.** Hacer ramificación de la señal mediante tendidos de red cortos para llegar al usuario final garantizando la prestación del servicio, realizar el mantenimiento y corrección de fallas de servicio.

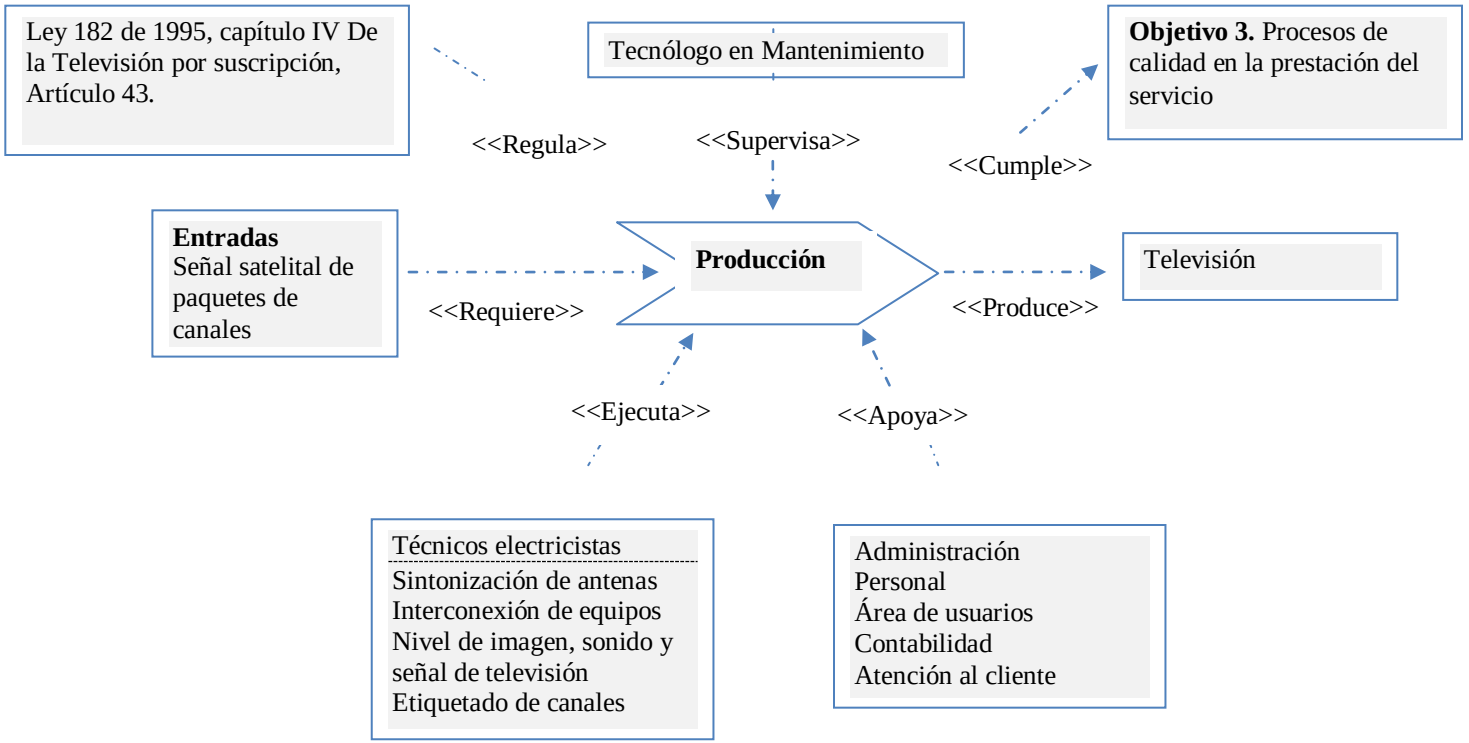
**Proceso de comercialización**

**Subproceso Servicio al usuario.** Gestionar las reclamaciones y atención a las solicitudes relacionadas con el servicio de televisión por los usuarios cumpliendo con los tiempos de respuesta, coordinar el proceso de inscripciones, pagos, cortes de servicio, ordenes de servicio y manejar una base de datos real de los usuarios existentes.

**Subproceso Facturación.** Mejorar los tiempos de distribución de recibos y aumentar el recaudo mensual.

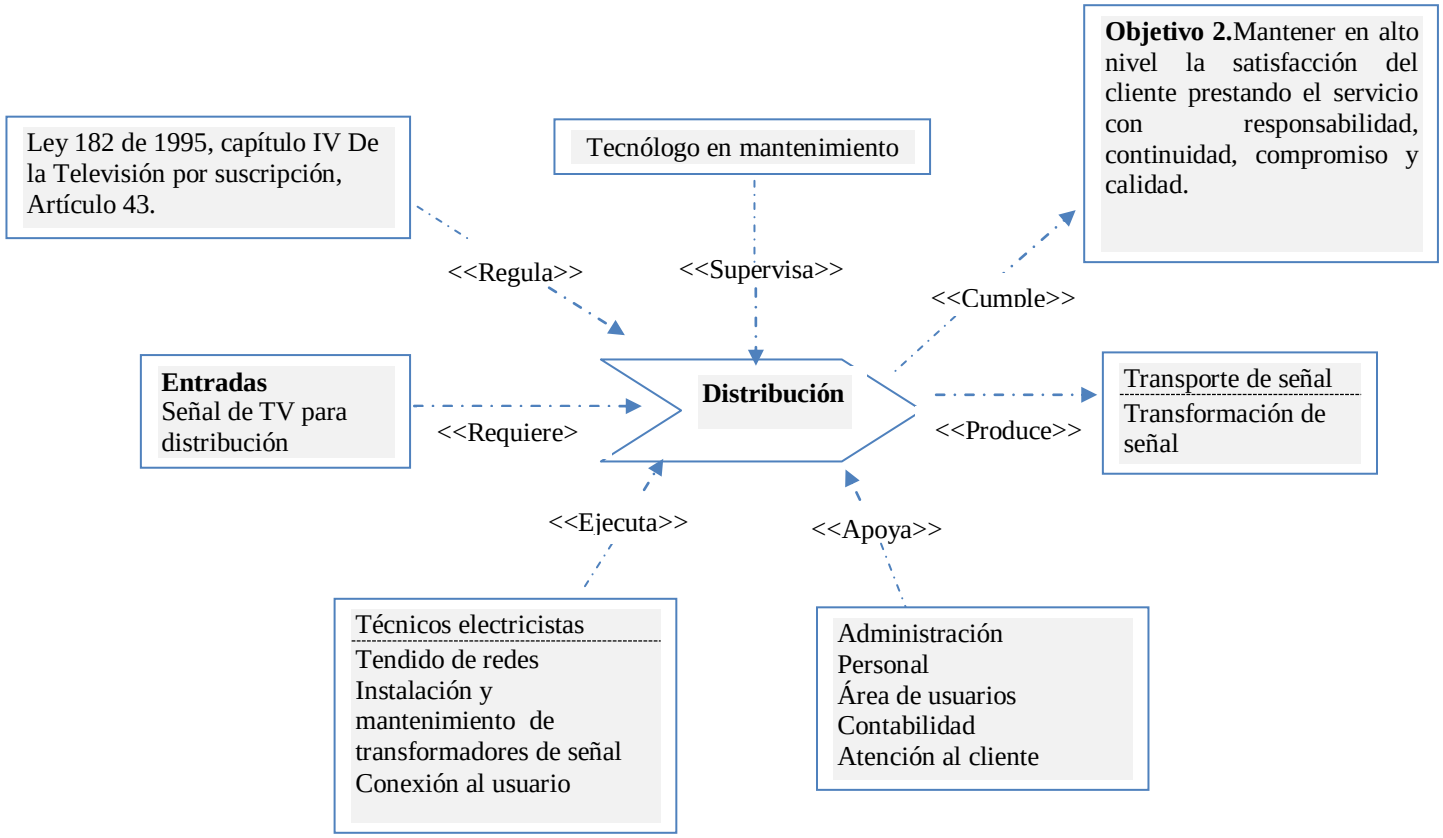
**Subproceso Control de acceso.** Servicio especial de canales que solo están disponibles para usuarios específicos, mediante este módulo se controlan los permisos de acceso a dichos canales, corte y reconexión del servicio.

**Figura 6.** PF Producción INGEPEC LTDA



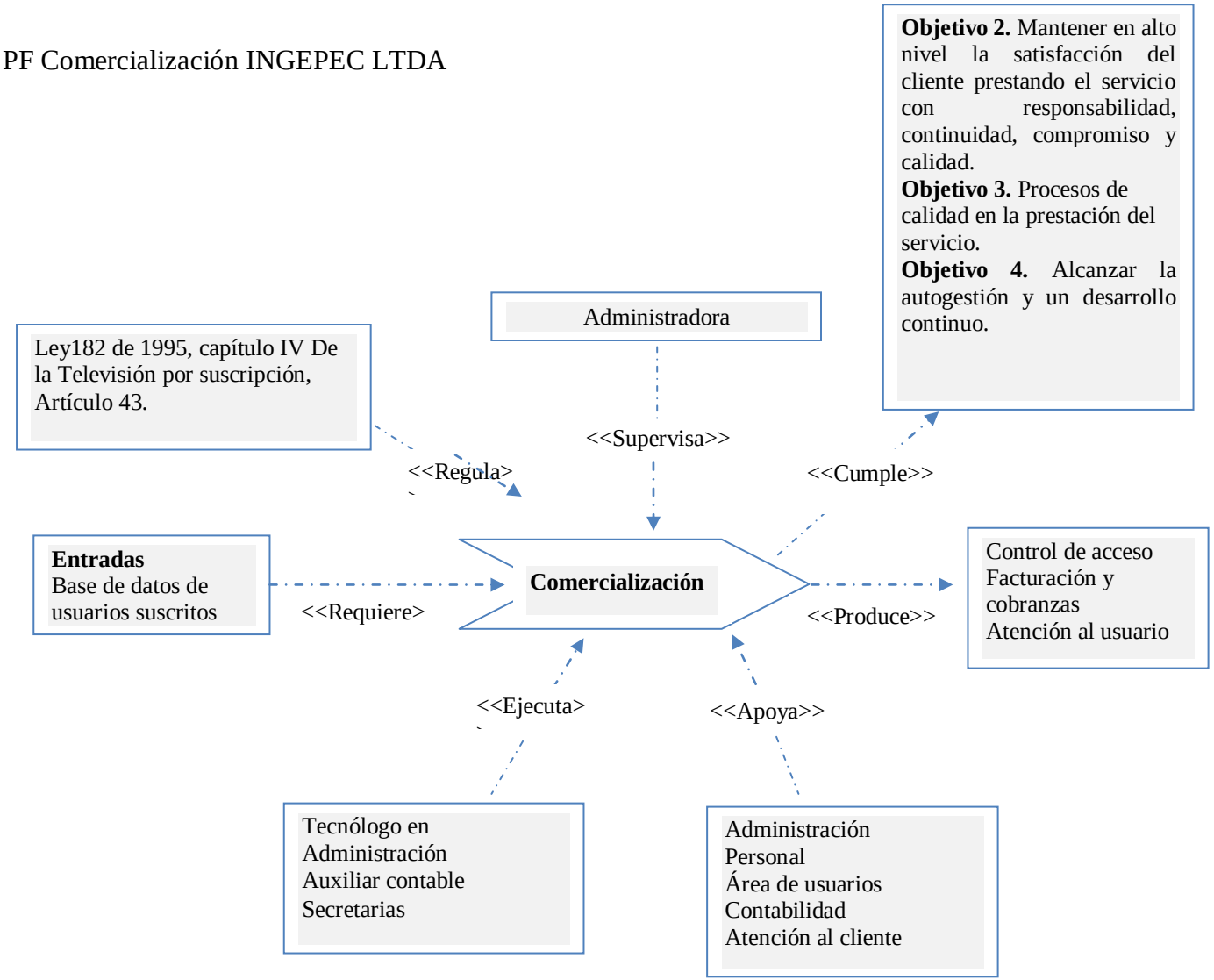

**Fuente**. Autores del proyecto

**Figura 7.** PF Distribución INGEPEC LTDA



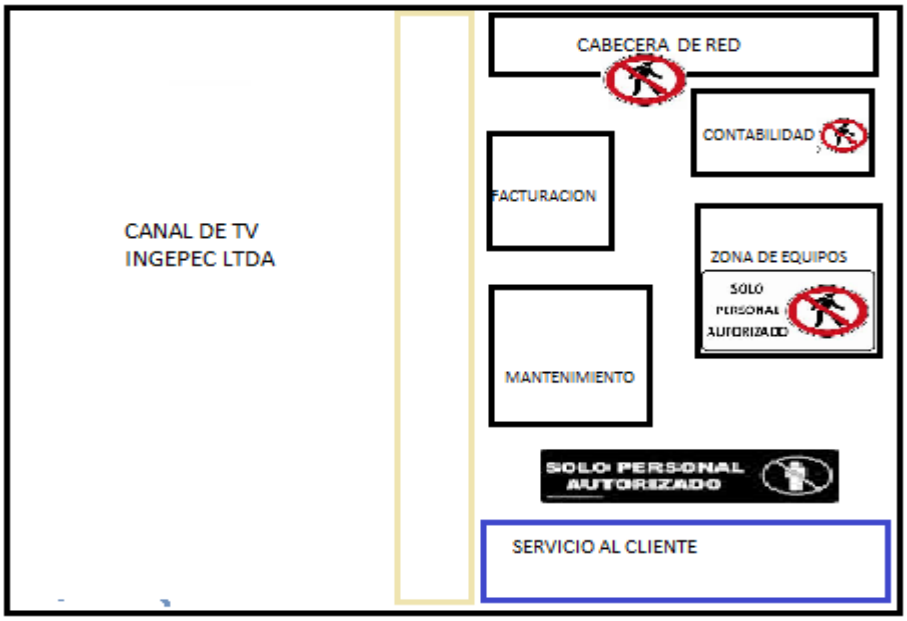

**Fuente**. Autores del proyecto

**Figura 8.** PF Comercialización INGEPEC LTDA




**Fuente**. Autores del proyecto

**Figura 9.** Estructura física de la empresa INGEPEC LTDA .




**Fuente**. Autores del proyecto

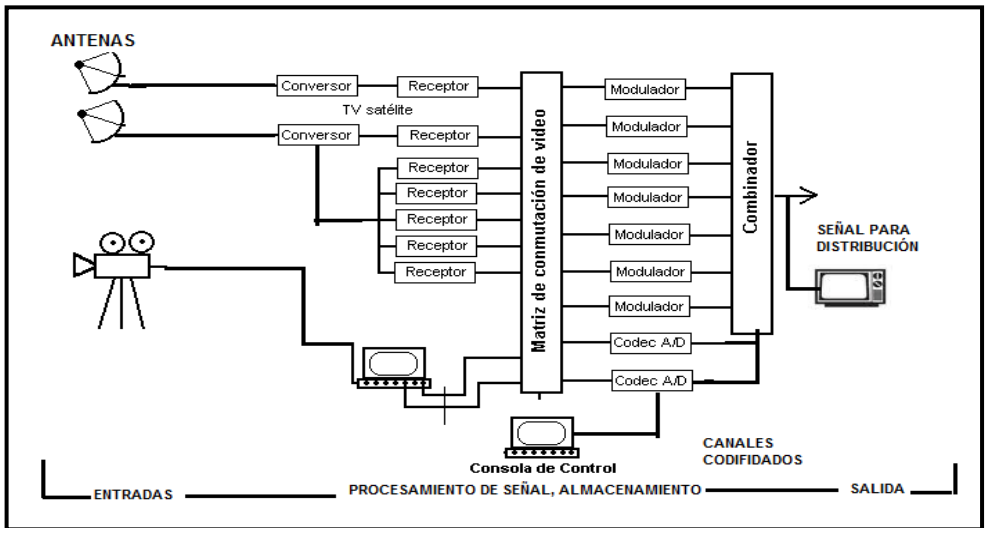
La empresa INGEPEC LTDA. físicamente se encuentra distribuida como aparece en la gráfica, en la entrada está ubicada el área de servicio al cliente, enseguida hay una zona de acceso restringida señalizada que no cuenta con mecanismos de protección, su ubicación no es la adecuada ya que por ahí debe ingresar todo el personal de la empresa para acceder al resto de las oficinas, luego sigue el área de Mantenimiento donde se realizan las reparaciones de los equipos y se ejecutan las órdenes de trabajo para realizar los mantenimientos de red. Continúa el área de la zona de equipos la cual se encuentra con acceso restringido pero sin controles efectivos, enseguida se encuentran el área de facturación, contabilidad y la cabecera de red, esta última cuenta con acceso restringido sin controles eficientes.

**Tecnologías de la información y las comunicaciones en INGEPEC LTDA .**Sistemas de Información. INGEPEC LTDA ., cuenta con sistemas de información para el proceso de contabilidad (Visual TNS), en el proceso de comercialización con un sistema de Facturación y de Usuarios.

Infraestructura Tecnológica. La empresa para el desarrollo del proceso de producción y comercialización cuenta con la siguiente infraestructura

El proceso Producción de señal en sus tres subprocesos (sintonización, modulación y multiplexación) cuenta con una infraestructura de Red llamada Cabecera.

**Figura10.** Cabecera de Red de televisión por cable




**Fuente**. Autores del proyecto

En la figura se observa el sistema de información de Producción de televisión por cable (CATV) en la cual se observa.

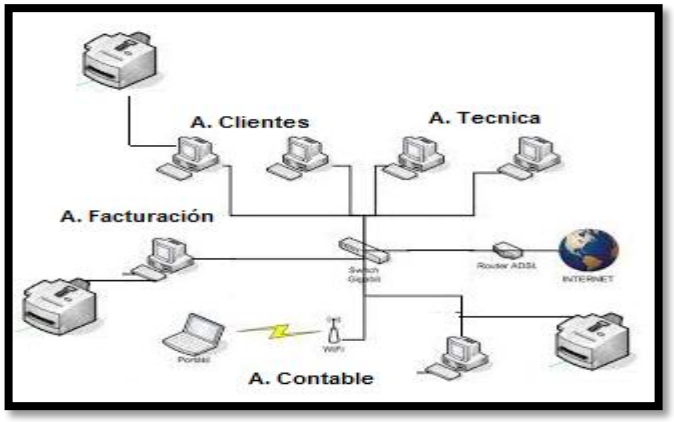
**Elementos de entrada de información:** antenas y cámaras de video.

**Elementos de procesamiento de señal:** receptores, conmutadores, moduladores, decodificadores y combinadores.

**Elementos de salida:** monitores y televisores.

El proceso comercialización se apoya de la siguiente infraestructura:

**Figura 11.** Infraestructura de Red proceso comercialización




**Fuente**. Autores del proyecto

Para el funcionamiento del área comercial la empresa cuenta con 7 computadores, 6 de escritorio interconectados por una red LAN mediante un SWITCH de 8 puertos y un computador portátil mediante un router Access Point WIFI que es el elemento que permite expansión de la red; además cada área cuenta con una impresora mediante conexión directa.

**Análisis de los activos y recursos.** Para el desarrollo del presente diagnostico se hizo necesario identificar los activos y recursos con que cuenta la empresa, con el fin de dimensionar el tamaño de la información y equipos existentes, estableciendo lo siguiente.

**Cuadro 5.** Recursos físicos: Inventario de Hardware

| NÚM. | EQUIPO | MARCA | NÚM. INVENTARIO | CARACTERISTICAS |
|---|---|---|---|---|
| 1 | Router | Linksys | H-0002-2 | ADSL |
| 2 | Computador | IBM | H-1020-2 | Pentium 4 |
| 3 | Computador | ACER | H-2002-2 | CORE DUO |
| 4 | Computador | ACER | H-0002-2 | CORE I7 |
| 5 | Computador | IBM | H-1012-2 | CORE DUO |
| 6 | Computador | SONY | H-0392-2 | CORE I3 |

**Fuente**. Autores del proyecto

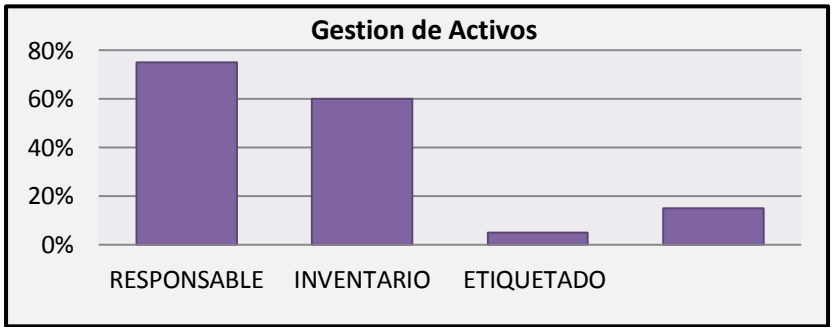
**Cuadro 6.** Inventario de Software(Herramientas para el manejo de información)

| SOFTWARE | VERSION | NUM. INVENTARIO | LICENCIAS | PRESENTACION | ASIGNADO A |
|---|---|---|---|---|---|
| Windows | XP | 10 4244-1 | 1 | CD-ROM | Contabilidad |
| Windows | 7 | 10 4244-2 | 1 | CD-ROM | Facturación |
| Office | 2007 | 10 4244-2 | 4 | CD-ROM | Servicio al Usuario |
| TNS | 2007 | 10 4244-3 | 1 | CD-ROM | Contabilidad |

**Fuente**. Autores del proyecto

**4.1.3 Análisis de la gestión de activos.** La gestión de activos permite a la empresa INGEPEC LTDA contar con estrategias para controlar mejor sus activos y mejorar su ciclo de vida.

**Grafico 7.** Análisis de la gestión de activos INGEPEC LTDA




**Fuente**. Autores del proyecto

En esta grafica se observa que la empresa INGEPEC LTDA , cuenta con un responsable del manejo de sus activos, función que se encuentra a cargo del administrador quien se apoya delegando actividades específicas a los jefes del área de producción, distribución y comercialización, siendo estos los responsables de los activos del área respectiva; a su vez se identifican todos los activos y se les asigna la responsabilidad por el mantenimiento y los controles apropiados, sin embargo existen activos que no cuentan con un propietario nombrado, es decir que están sin ninguna protección. Para el manejo de inventario lo realiza la auxiliar contable a través de un software y conteo físico, identificando y documentado todos los activos con que cuenta la empresa con el fin de tener una protección efectiva sobre los mismos, cabe mencionar que este inventario no se realiza permanentemente, sino cuando lo requieren los administrativos de la empresa. INGEPEC LTDA tiene establecida como regla para el uso aceptable de los activos el etiquetado de los mismos, permitiendo identificar cuales empleados usan o tienen acceso a los activos de la empresa y de esta manera conocer los responsables del uso que le den a los recursos; como se observa en la gráfica el porcentaje es interior al 20% lo que indica que este aspecto es poco controlado debido a que no todos los activos están etiquetados.

**4.1.4 Caracterización de la información de INGEPEC LTDA.** La empresa maneja información de diferentes tipos la cual es administrada de acuerdo a su nivel de importancia, se puede identificar las siguientes.

**Información Administrativa.** Cuando se habla de información de tipo administrativo es la que tiene que ver con el desarrollo de objetivos misionales, manejo de la empresa, gerencia, socios, estrategias de ventas y políticas; ésta es manejada estrictamente por personal de confianza a través del gerente y de la administradora.

**Información contable**. Es toda la información financiera y económica de la empresa la cual es manejada a través del software contable Visual TNS, adicional a esto se maneja un software de facturación y uno de inventarios. Estos datos son administrados por la contadora de la empresa.

**Información de usuarios.** Contiene toda la información de los clientes de la empresa tales como nombre, cedula, dirección, teléfonos, fecha de afiliación al servicio de televisión, fecha de retiros o cambios de residencia, servicios técnicos brindados , valor del plan básico mensual que maneja y otros datos de tipo informativo. La base de datos de usuarios es administrada por el área de facturación.

**Información técnica del servicio de televisión**. Todo lo referente a la ubicación de los diferentes satélites que proveen los canales de tv que son difundidos a los usuarios, configuración de los equipos receptores y decodificadores de video, parámetros de medición y calibración de los equipos de modulación y de red de distribución de la señal que llega al usuario final, archivos de actualización de los equipos codificadores de señal de video.

**Información de proveedores de servicio.** Contiene todos los datos de los propietarios de canales de televisión a quienes se les compra dicho servicio para que los canales privados puedan ser vistos en la ciudad de Ocaña a través de la televisión por cable. Se registran datos como teléfonos de contactos, privilegios otorgados a la empresa, promociones y valores cobrados por cada usuario. Toda la información mencionada anteriormente es de estricta reserva teniendo en cuenta que es relevante para la competencia.

**4.1.5 Auditoría realizada a la seguridad física de la empresa INGEPEC LTDA.** Realizada la auditoria para evaluar la seguridad física y del entorno de la empresa INGEPEC LTDA se obtuvieron los siguientes hallazgos:

Revisado el perímetro de seguridad física se evidencia que el área de producción no cuenta con este tipo de seguridad definida en la cabecera de red, lo cual puede ocasionar vulnerabilidad de la información, perdida o daño de equipos y robo de señal; por su parte el área de servicio al usuario presenta deficiencia en la seguridad física, puesto que no existen barreras blindadas ni personal de vigilancia privada que evite riesgos como pérdida de activos y manipulación de la información.

Por otro lado, luego de verificar los controles de ingreso físico a las áreas de acceso restringidas se evidencia que el área de producción utiliza como control de acceso solo la bitácora que contiene datos de la persona que ingresa como nombre, cargo, fecha, hora de entrada, hora de salida y observación, sin embargo al revisarla se puede constatar que este control no es efectivo porque no se cumple con la actualización de la misma, generando que no se pueda detectar el personal que ingresa a las áreas de acceso restringido lo que impide identificar responsables de posibles eventos que ocasionen daño o interferencia en la información y fallas en la prestación del servicio; además las cerraduras de las puertas no son seguras, lo que origina que cualquier persona pueda manipular los equipos y acceder a la información procesada en el área.

Posteriormente, se examinó la seguridad del cableado de la energía y las telecomunicaciones encontrando que los tendidos de cable no cuentan con etiquetado que permita su fácil identificación, no existe protección en los tendidos de cable mediante parrillas o canaletas y los cableados de distribución se encuentran a la vista lo que facilita su intercepción; esto se debe a que no hubo planeación en el momento del tendido del cableado. Además se evidencia que los controles de corte y re-conexión del servicio no son efectivos porque no existen decodificadores por usuarios que permitan administrar adecuadamente la prestación del servicio. (Ver anexos C,D,E,F,G,H,I,J,K,L,M,N,O,P)

**4.1.6 Análisis y evaluación de riesgos.** Los riesgos son eventos negativos internos y externos que se pueden presentar afectando alcanzar los objetivos de la organización; su evaluación debe identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del mismo y los objetivos relevantes para la organización y los resultados deben guiar y determinar la acción de gestión apropiada para implementar los controles seleccionados y proteger la información contra riesgos.

En la empresa INGEPEC LTDA se evidencia que no existe la identificación y análisis de los riesgos, por lo que no cuentan con controles eficientes establecidos que les permita proteger sus activos de los eventos que pueden afectar el cumplimiento de los objetivos.

**Cuadro 7**. Matriz de Riesgos INGEPEC LTDA

| **INGEPEC LTDA<br>MATRIZ DE RIESGOS** | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Objetivo.** Identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del mismo y los objetivos relevantes para la empresa INGEPEC LTDA | | | | | | | | | | | | | | | | | | |
| **IDENTIFICACIÓN DE RIESGOS** | | | | | **ANALISIS CUALITATIVO DE LOS RIESGOS** | | | | | | | | | | | | | **PLANIFICACION DE LA RESPUESTA A LOS RIESGOS** |
| *** CÓD DE LRIESGO** | **PROCESO** | **RIESGO** | **CAUSA** | **DESCRIPCIÓN DEL RIESGO** | **PROBABILIDAD** | | | | | **IMPACTO** | | | | | **CALIFICACION DEL RIESGO** | | | **ESTRATEGIAS/ CONTINGENCIAS** |
| | | | | | Muy probable | Bastante Probable | Probable | Poco Probable | Improbable | Muy Alto | Alto | Moderado | Bajo | Muy Bajo | Alto | Moderado | Bajo | |
| | | | | | **0.9** | **0.7** | **0.5** | **0.3** | **0.1** | **0.8** | **0.4** | **0.2** | **0.1** | **0.05** | | | | |
| RO | Producción | Pérdida, daño e interferencia de la información por el acceso físico no autorizado. | 1. No existen controles de entrada apropiados.<br><br>2. No existen un empleado que vigile el ingreso a esta área<br><br>3. Las puertas para el ingreso al área no tienen mecanismos de control de seguridad.<br><br>4. El área donde se encuentran instalados los equipos de transmisión de señal no cuenta con la política de acceso restringid | Si no se cuenta con perímetros de seguridad para proteger las áreas que contienen información se pueden presentar pérdida, daño e interferencia de la misma debido al ingreso de personal no autorizado. | **X** | | | | | **X** | | | | | **0.72** | | | **Aceptar/** Definir el perímetro de seguridad para proteger las áreas de procesamiento de información, a través de barreras o medidas de control físicas en las instalaciones de la empresa. |

Cuadro 7. (Continuación)

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | o.<br><br>5. No se actualiza la bitácora.<br><br>6. No existe control de acceso físico al área. | | | | | | | | | | | | | |
| RT | | Robo o pérdida de señal por la intercepción del cableado de las redes de TV | 1. Falta de planeación al realizar el tendido del cableado presentando inconvenientes para su identificación y protección. | Si no se cuenta con la seguridad del cableado de las redes de TV se puede presentar intercepción del mismo por personal no autorizado debido a que no se cuenta con controles eficientes. | | **X** | | | | **X** | | | | | **0.56** | **Aceptar/** Proteger el cableado de TV contra intercepción o daño mediante el resguardo en canaletas. |
| RO | Comercialización | Pérdida de la información por el acceso físico no autorizado. | 1. No existen barreras blindadas que aseguren el área de servicio al cliente, ni se cuenta con personal de vigilancia privada. | Si no se cuenta con controles físicos de entrada apropiados para proteger las áreas que contienen información se puede presentar pérdida de la misma, debido a que el área de servicio al cliente en la cual se reciben pagos en efectivo presenta deficiencia en la seguridad física. | | | **X** | | | **X** | | | | | **0.40** | **Aceptar/** Implementar sistemas biométricos de control de acceso a las áreas no autorizadas, con el fin de tener registro físico, fecha, hora de ingreso y salida, datos de la persona que ingresa y de esta manera monitorear que sol ingrese personal autorizado. |

**Fuente**. Autores del proyecto

Código identificador del riesgo. Permite trabajar de forma estandarizada y ser incluido en una base de datos de riesgos.

RO - Riesgo Organizacional

RT - Riesgo Técnico
RA - Riesgo Administrativo
RE - Riesgo Externo

**Cuadro 8.** Ayuda para interpretación de matriz de riesgo.

| PROBABILIDAD | CUANTIFICACIÓN | DESCRIPCIÓN | FRECUENCIA |
|---|---|---|---|
| Muy probable | 0.9 | Se espera que el evento ocurra en la mayoría de los casos. | Más de 1 vez al año. |
| Bastante Probable | 0.7 | El evento probablemente ocurrirá. | Al menos 1 vez en el último año. |
| Probable | 0.5 | El evento puede suceder eventualmente. | Al menos 1 vez en los últimos 2 años. |
| Poco Probable | 0.3 | El evento podría ocurrir en algún momento y se considera que es difícil que suceda. | Al menos 1 vez en los últimos 5 años. |
| Improbable | 0.1 | El evento ocurriría solamente en circunstancias excepcionales. | No se ha presentado en los últimos 5 años. |

**Fuente**. Autores del proyecto

**Cuadro 9.** Calificación dada en la matriz de riesgo.

| IMPACTO | CUANTIFICACIÓN | DESCRIPCIÓN |
|---|---|---|
| Muy Alto | 0.8 | - Pérdida de la capacidad de operación que tiene efectos perjudiciales.<br>- Enorme pérdida financiera.<br>- Grave pérdida de imagen. |
| Alto | 0.4 | - Daños extensivos, pérdida de la capacidad de operación que no tienen efectos perjudiciales.<br>- Pérdidas financieras mayores.<br>- Pérdida de imagen. |
| Moderado | 0.2 | - Se necesita asistencia de un tercero para subsanar los daños.<br>- La pérdida financiera es alta.<br>- Podría existir pérdida de imagen. |
| Bajo | 0.1 | - Se puede subsanar los daños inmediatamente.<br>- La pérdida financiera es media.<br>- No hay pérdida de imagen. |
| Muy Bajo | 0.05 | - No hay daños o perjuicios.<br>- La pérdida financiera es baja.<br>- No hay pérdida de imagen. |

**Fuente**. Autores del proyecto

**Cuadro 10.** Evaluación, marcador de riesgo para un riesgo específico (PxI)

| IMPACTO / PROBABILIDAD / PROBABILIDAD | Muy bajo 0.05 | Bajo 0.1 | Moderado 0.2 | Alto 0.4 | Muy Alto 0.8 |
|---|---|---|---|---|---|
| Muy Probable 0.9 | 0.05 | 0.09 | 0.18 | 0.36 | 0.72 |
| Bastante Probable 0.7 | 0.04 | 0.07 | 0.14 | 0.28 | 0.56 |
| Probable 0.5 | 0.03 | 0.05 | 0.10 | 0.20 | 0.40 |
| Poco Probable 0.3 | 0.02 | 0.03 | 0.06 | 0.12 | 0.24 |
| Improbable 0.1 | 0.01 | 0.01 | 0.02 | 0.04 | 0.08 |

| | | |
|---|---|---|
| **Riesgo Bajo** | | Gestionar mediante procedimientos de rutina, es improbable que se necesite la aplicación específica de recursos. |
| **Riesgo Moderado** | | Gestionar mediante procedimientos de monitoreo o respuesta específicas. |
| **Riesgo Alto** | | Acción inmediata, especificar planes de acción y atención de la alta dirección. |

**Fuente**. Autores del proyecto

**4.1.7 Resultados del diagnóstico de la seguridad física en la empresa INGEPEC LTDA.** De acuerdo a lo expuesto anteriormente y a las evidencias encontradas se detectó que el espacio físico se encuentra mal distribuido ya que para acceder al área de mantenimiento se tiene acceso al área de contabilidad y facturación en donde no existen cubículos ni barreras que independicen la oficina dejando expuesta la documentación y equipos; además se evidenció que existen puertas en madera y las metálicas tienen cerraduras mecánicas que pueden ser manipuladas fácilmente, exponiendo la información a pérdida o robo por parte de personal de la empresa o terceros, debido a que no se cuenta con controles efectivos como los sistemas biométricos, que permiten tener registro de las entradas y salidas a la empresa evidenciando los posibles eventos que puedan ocurrir; por otra parte el área de producción tiene fácil acceso por parte de cualquier persona ya que se encuentra ubicada en un sótano en donde no se puede evidenciar el ingreso del personal encargado de la administración de los equipos ni sus movimientos al interior de la misma y tienen como control de entrada la bitácora la cual se encuentra desactualizada, dejando la información sin ninguna protección adecuada.

Lo anteriormente evidenciado en cuanto a seguridad física conlleva a que la información de la empresa INGEPEC LTDA sea vulnerable por cualquier incidente afectando su integridad, disponibilidad y confidencialidad.

Cuando se habla de integridad de la información se hace referencia a que no se realicen modificaciones a los datos, información o procesos por personas autorizadas y no autorizadas y que estos sean consistentes tanto interna como externamente.

En la empresa INGEPEC LTDA la integridad de la información puede ser afectada cuando por accidente o con mala intención se modifican o borran los datos importantes que son parte de la información de la empresa, teniendo en cuenta que cualquier persona puede acceder al espacio físico y por ende a la información.

La información es disponible cuando se puede acceder a ella de manera confiable y oportuna por el personal que la requiera para toma de decisiones; por lo que al no contar con controles de acceso de entrada adecuados la empresa corre el riesgo de pérdida o daño en equipos, lo que puede ocasionar que la información no pueda estar disponible cuando sea necesaria.

La confidencialidad es una característica de la información muy importante y aún más en la empresa INGEPEC donde se administra una gran base de datos de clientes potenciales en Ocaña siendo esta significativa para la competencia, razón por la cual la empresa debe prevenir el acceso no autorizado ya sea en forma intencional o no intencional a la información con la implementación de controles efectivos que eviten la manipulación o pérdida de la misma.

## 4.2 IDENTIFICACION Y ANALISIS DE LOS COMPONENTES QUE INTEGRAN EL PLAN DE GESTIÓN DE SEGURIDAD PARA LA EMPRESA INGEPEC LTDA DE ACUERDO A LAS NORMAS ISO/IEC 27001 Y 27002.

El plan de gestión de seguridad de la información permite diseñar una mejor forma de manejar y coordinar las actividades a corto y largo plazo, incluyendo métodos y estrategias que aborden los aspectos necesarios para una correcta administración de la información, es importante resaltar que el plan de gestión marca las pautas a seguir y cómo debe hacerse; razón por la cual debe estar elaborado coherentemente a las necesidades de la empresa y debe ser claro conciso y preciso para evitar desviaciones en el cumplimiento del mismo.

De acuerdo a lo anterior se define una estructura lógica para el plan de gestión de la empresa INGEPEC LTDA que facilita su análisis y a su vez que es entendible a todo el personal que labora en la organización.

### 4.2.1 Estructura Del Plan De Gestión

**Objetivo del plan de gestión.** Debe ser claro y que indique específicamente que se lograra, permitirá identificar el resultado final que se pretende alcanzar.

**Alcance.** En el alcance determinara las normas bajo las que se elaborara el plan de gestión de seguridad de la información, a su vez describirá aspectos como estrategias y limitaciones, tiempo y encargados de la implementación.

**Responsables.** En este aspecto se definirán los responsables de la elaboración del plan de gestión, identificando quien será encargado de su implementación, definiendo el encargado de la supervisión, actualización y evaluación; con el fin de asignar responsabilidades y funciones que den cumplimiento a lo planteado.

**Recursos.** Se incluyen los recursos necesarios con el fin de adecuar las necesidades para que se de disponibilidad presupuestal a los requerimientos económicos, físicos y humanos que se estiman para el plan de gestión de seguridad.

**Estrategias.** Se especificara claramente en qué consiste cada política para gestionar la seguridad de la información y como se debe realizar. Se indicaran los lineamientos para que INGEPEC LTDA alcance un nivel de seguridad adecuado y minimice los riesgos y amenazas existentes.

**Actividades.** Tomando como base una norma de seguridad de la información se indicará la política para dar cumplimiento a cada criterio establecido en la misma, realizando actividades coherentes a los requerimientos de la empresa, la cual estará diseñada de la siguiente manera

**4.2.2 Criterios Normativos Para El Plan De Gestión De INGEPEC LTDA .**Analizando las normas existentes relacionadas con la seguridad de la información, se determina que el proyecto se realiza con base en las normas ISO/IEC 27001 e ISO/IEC 27002 que es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información y sirve como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas.

La norma ISO/IEC 27002, establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos de control y los controles son implementados para satisfacer los requerimientos identificados por una evaluación del riesgo.

La norma ISO/IEC 27002 contiene 11 dominios, 39 objetivos de control y 133 controles de seguridad.

**Grafico 8.** Contenido norma ISO/IEC 27002

ISO/IEC 27002:2005. Dominios (11), Objetivos de control (39) y Controles (133)

CLIC SOBRE CADA CONTROL PARA MÁS INFORMACIÓN

Versión actualizada de esta lista en: http://www.iso27000.es/download/Controles-ISO27002-2005.pdf

5. POLÍTICA DE SEGURIDAD.
5.1 Política de seguridad de la información.
5.1.1 Documento de política de seguridad de la información.
5.1.2 Revisión de la política de seguridad de la información.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
6.1 Organización interna.
6.1.1 Compromiso de la Dirección con la seguridad de la información.
6.1.2 Coordinación de la seguridad de la información.
6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
6.1.5 Acuerdos de confidencialidad.
6.1.6 Contacto con las autoridades.
6.1.7 Contacto con grupos de especial interés.
6.1.8 Revisión independiente de la seguridad de la información.
6.2 Terceros.
6.2.1 Identificación de los riesgos derivados del acceso de terceros.
6.2.2 Tratamiento de la seguridad en la relación con los clientes.
6.2.3 Tratamiento de la seguridad en contratos con terceros.
7. GESTIÓN DE ACTIVOS.
7.1 Responsabilidad sobre los activos.
7.1.1 Inventario de activos.
7.1.2 Propiedad de los activos.
7.1.3 Uso aceptable de los activos.
7.2 Clasificación de la información.
7.2.1 Directrices de clasificación.
7.2.2 Etiquetado y manipulado de la información.
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
8.1 Antes del empleo.
8.1.1 Funciones y responsabilidades.
8.1.2 Investigación de antecedentes.
8.1.3 Términos y condiciones de contratación.
8.2 Durante el empleo.
8.2.1 Responsabilidades de la Dirección.
8.2.2 Concienciación, formación y capacitación en seg. de la informac.
8.2.3 Proceso disciplinario.
8.3 Cese del empleo o cambio de puesto de trabajo.
8.3.1 Responsabilidad del cese o cambio.
8.3.2 Devolución de activos.
8.3.3 Retirada de los derechos de acceso.
9. SEGURIDAD FÍSICA Y DEL ENTORNO.
9.1 Áreas seguras.
9.1.1 Perímetro de seguridad física.
9.1.2 Controles físicos de entrada.
9.1.3 Seguridad de oficinas, despachos e instalaciones.
9.1.4 Protección contra las amenazas externas y de origen ambiental.
9.1.5 Trabajo en áreas seguras.
9.1.6 Áreas de acceso público y de carga y descarga.
9.2 Seguridad de los equipos.
9.2.1 Emplazamiento y protección de equipos.
9.2.2 Instalaciones de suministro.
9.2.3 Seguridad del cableado.
9.2.4 Mantenimiento de los equipos.
9.2.5 Seguridad de los equipos fuera de las instalaciones.
9.2.6 Reutilización o retirada segura de equipos.
9.2.7 Retirada de materiales propiedad de la empresa.
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.
10.1 Responsabilidades y procedimientos de operación.
10.1.1 Documentación de los procedimientos de operación.
10.1.2 Gestión de cambios.
10.1.3 Segregación de tareas.
10.1.4 Separación de los recursos de desarrollo, prueba y operación.
10.2 Gestión de la provisión de servicios por terceros.
10.2.1 Provisión de servicios.
10.2.2 Supervisión y revisión de los servicios prestados por terceros.
10.2.3 Gestión del cambio en los servicios prestados por terceros.
10.3 Planificación y aceptación del sistema.
10.3.1 Gestión de capacidades.
10.3.2 Aceptación del sistema.
10.4 Protección contra el código malicioso y descargable.
10.4.1 Controles contra el código malicioso.
10.4.2 Controles contra el código descargado en el cliente.
10.5 Copias de seguridad.
10.5.1 Copias de seguridad de la información.
10.6 Gestión de la seguridad de las redes.
10.6.1 Controles de red.
10.6.2 Seguridad de los servicios de red.
10.7 Manipulación de los soportes.
10.7.1 Gestión de soportes extraíbles.
10.7.2 Retirada de soportes.
10.7.3 Procedimientos de manipulación de la información.
10.7.4 Seguridad de la documentación del sistema.
10.8 Intercambio de información.
10.8.1 Políticas y procedimientos de intercambio de información.
10.8.2 Acuerdos de intercambio.
10.8.3 Soportes físicos en tránsito.
10.8.4 Mensajería electrónica.
10.8.5 Sistemas de información empresariales.
10.9 Servicios de comercio electrónico.
10.9.1 Comercio electrónico.
10.9.2 Transacciones en línea.
10.9.3 Información públicamente disponible.
10.10 Supervisión.
10.10.1 Registros de auditoría.
10.10.2 Supervisión del uso del sistema.
10.10.3 Protección de la información de los registros.
10.10.4 Registros de administración y operación.
10.10.5 Registro de fallos.
10.10.6 Sincronización del reloj.
11. CONTROL DE ACCESO.
11.1 Requisitos de negocio para el control de acceso.
11.1.1 Política de control de acceso.
11.2 Gestión de acceso de usuario.
11.2.1 Registro de usuario.
11.2.2 Gestión de privilegios.
11.2.3 Gestión de contraseñas de usuario.
11.2.4 Revisión de los derechos de acceso de usuario.
11.3 Responsabilidades de usuario.
11.3.1 Uso de contraseñas.
11.3.2 Equipo de usuario desatendido.
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
11.4 Control de acceso a la red.
11.4.1 Política de uso de los servicios en red.
11.4.2 Autenticación de usuario para conexiones externas.
11.4.3 Identificación de los equipos en las redes.
11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
11.4.5 Segregación de las redes.
11.4.6 Control de la conexión a la red.
11.4.7 Control de encaminamiento (routing) de red.
11.5 Control de acceso al sistema operativo.
11.5.1 Procedimientos seguros de inicio de sesión.
11.5.2 Identificación y autenticación de usuario.
11.5.3 Sistema de gestión de contraseñas.
11.5.4 Uso de los recursos del sistema.
11.5.5 Desconexión automática de sesión.
11.5.6 Limitación del tiempo de conexión.
11.6 Control de acceso a las aplicaciones y a la información.
11.6.1 Restricción del acceso a la información.
11.6.2 Aislamiento de sistemas sensibles.
11.7 Ordenadores portátiles y teletrabajo.
11.7.1 Ordenadores portátiles y comunicaciones móviles.
11.7.2 Teletrabajo.
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.
12.1 Requisitos de seguridad de los sistemas de información.
12.1.1 Análisis y especificación de los requisitos de seguridad.
12.2 Tratamiento correcto de las aplicaciones.
12.2.1 Validación de los datos de entrada.
12.2.2 Control del procesamiento interno.
12.2.3 Integridad de los mensajes.
12.2.4 Validación de los datos de salida.
12.3 Controles criptográficos.
12.3.1 Política de uso de los controles criptográficos.
12.3.2 Gestión de claves.
12.4 Seguridad de los archivos de sistema.
12.4.1 Control del software en explotación.
12.4.2 Protección de los datos de prueba del sistema.
12.4.3 Control de acceso al código fuente de los programas.
12.5 Seguridad en los procesos de desarrollo y soporte.
12.5.1 Procedimientos de control de cambios.
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
12.5.3 Restricciones a los cambios en los paquetes de software.
12.5.4 Fugas de información.
12.5.5 Externalización del desarrollo de software.
12.6 Gestión de la vulnerabilidad técnica.
12.6.1 Control de las vulnerabilidades técnicas.
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
13.1 Notificación de eventos y puntos débiles de seguridad de la información.
13.1.1 Notificación de los eventos de seguridad de la información.
13.1.2 Notificación de puntos débiles de seguridad.
13.2 Gestión de incidentes y mejoras de seguridad de la información.
13.2.1 Responsabilidades y procedimientos.
13.2.2 Aprendizaje de los incidentes de seguridad de la información.
13.2.3 Recopilación de evidencias.
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
14.1.2 Continuidad del negocio y evaluación de riesgos.
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
14.1.4 Marco de referencia para la planificación de la cont. del negocio.
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.
15. CUMPLIMIENTO.
15.1 Cumplimiento de los requisitos legales.
15.1.1 Identificación de la legislación aplicable.
15.1.2 Derechos de propiedad intelectual (DPI).
15.1.3 Protección de los documentos de la organización.
15.1.4 Protección de datos y privacidad de la información de carácter personal.
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
15.1.6 Regulación de los controles criptográficos.
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.
15.2.1 Cumplimiento de las políticas y normas de seguridad.
15.2.2 Comprobación del cumplimiento técnico.
15.3 Consideraciones sobre las auditorías de los sistem. de información.
15.3.1 Controles de auditoría de los sistemas de información.
15.3.2 Protección de las herramientas de auditoría de los sist. de inform.

Documento sólo para uso didáctico. La norma oficial debe adquirirse en entidades autorizadas para su venta

Ver. 4.0, 16-1-2011

**Fuente**. ISO/IEC 27002:2005. Dominios, Objetivos de Control y Controles

Cada dominio contiene un número de objetivos de control de seguridad principales. Los once dominios (acompañados por el número de objetivos de control incluidos en cada dominio) son:

Política de seguridad (1)
Aspectos organizativos de la seguridad de la información (2)
Gestión de activos (2)
Seguridad ligada a los recursos humanos (3)
Seguridad física y del entorno (2)
Gestión de comunicaciones y operaciones (10)
Control de acceso (7)
Adquisición, desarrollo y mantenimiento de sistemas de información (6)
Gestión de incidentes en la seguridad de la información (2)
Gestión de la continuidad del negocio (2)
Cumplimiento (3)

Realizando un análisis detallado de la norma ISO/IEC 27002 y teniendo en cuenta las necesidades identificadas en la empresa INGEPEC LTDA , el diseño del plan de gestión de seguridad para controlar el acceso a las áreas restringidas de la empresa se define con base en lo siguiente:
Generalidades
Objetivos
Alcance
Políticas
Domino
Objetivos de control
Controles

**Cuadro 11.** Dominios Objetivos de Control y Controles empleados en este proyecto

| DOMINIOS | OBEJETIVOS DE CONTROL | CONTROLES |
|---|---|---|
| POLITICA DE SEGURIDAD | Política de Seguridad de la Información | Documento de la política de seguridad de la información |
| | | Revisión de la política de seguridad de la información |
| ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | Organización Interna | Compromiso de la Dirección con la seguridad de la información |
| | | Asignación de responsabilidades relativas a la seguridad de la información |
| | | Acuerdos de confidencialidad |
| GESTION DE ACTIVOS | Responsabilidad de los activos | Inventario de activos |
| | | Propiedad de los activos |
| | Clasificación de la información | Lineamientos de clasificación |
| SEGURIDAD LIGADA A LOS RECURSOS HUMANOS | Antes del empleo | Roles y responsabilidades |
| | | Investigación de Antecedentes |
| | | Términos y condiciones de empleo |
| | Durante el empleo | Concienciación, formación y capacitación en seguridad de la información |
| | Después del empleo | Retiro de los derechos de acceso |
| SEGURIDAD FÍSICA Y DEL ENTORNO | Áreas seguras | Perímetro de Seguridad. |
| | | Controles físicos de entrada |
| | Equipo de seguridad | Seguridad del cableado |
| GESTION DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACION | Gestión de incidentes y mejoras en la seguridad de la información | Responsabilidades y procedimientos. |
| | | Aprender de los incidentes ocurridos en la seguridad de la información |
| GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | Aspectos de seguridad de la información en la gestión de la continuidad del negocio | Continuidad del negocio y evaluación de riesgos. |
| CUMPLIMIENTO | Cumplimiento de los objetivos | Identificación de la legislación aplicable |

**Fuente**. Autores del proyecto

Los dominios seleccionados para el plan de gestión de seguridad de la empresa INGEPEC LTDA fueron escogidos tomando como base las definiciones de los mismos y su aplicabilidad al control del acceso físico.

**Política de seguridad.** Este dominio le suministra a la empresa el documento que proporcionará a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales, las leyes y regulaciones relevantes; su importancia radica en que a través del mismo se dan los lineamientos para proteger la información de amenaza con el fin de garantizar la continuidad de los sistemas y la operación de la empresa.

**Organización de la seguridad de la información.** Orientado a administrar la seguridad de la información dentro de la empresa y establecer un marco gerencial para controlar su implementación. Este dominio le ayuda a INGEPEC a que haya un compromiso por parte de la dirección en la asignación de roles y responsabilidades de la seguridad de la información y apoyo para las iniciativas de la misma.

**Gestión de Activos.** Mediante este dominio se pretende que la empresa tenga en cuenta que debe lograr y mantener una adecuada protección de los activos de la misma y a su vez gestionar diariamente estrategias que faciliten dicha tarea, estas estrategias deben estar ligadas con los inventarios de los activos y el control para lograr una adecuada administración por parte del personal de los recursos físicos evitando el daño y la pérdida de los mismos que afectan el capital empresarial.

**Seguridad ligada a los recursos humanos.** Dominio que está orientado a reducir los riesgos de error humano y uso inadecuado de las instalaciones; para INGEPEC LTDA es importante porque a través del mismo se busca asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles en los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de la información.

**Seguridad física y del entorno.** A través de este dominio se busca impedir accesos no autorizados, daños e interferencia a las instalaciones e información de la empresa. Este dominio es importante debido a que es la mayor debilidad que presenta la empresa INGEPEC y es el tema central del presente proyecto, su aplicabilidad evita el máximo riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad y áreas protegidas facilitando la implementación de controles de acceso efectivos.

**Gestión de incidentes en la seguridad de la información.** Orientado a administrar todos los eventos que atentan contra la confidencialidad, integridad y disponibilidad de la información y los activos tecnológicos. Para INGEPEC LTDA es importante el uso de este dominio puesto que le permite establecer las responsabilidades y procedimientos para manejar de manera efectiva los eventos y debilidades en la seguridad de la información una vez que han sido reportados.

**Gestión de la continuidad del negocio.** Es relevante incluir este dominio teniendo en cuenta que le ayudara a INGEPEC LTDA a implementar el proceso de gestión de la continuidad del negocio para minimizar el impacto sobre la organización y recuperarse de las pérdidas de activos de información hasta un nivel aceptable a través de una combinación de controles preventivos y de recuperación.

**Cumplimiento.** Este dominio es supremamente relevante que se tenga en cuenta, puesto que permite evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad, de misma manera al sr INGEPEC LTDA una empresa vigilada por la ANTV debe cumplir la normatividad que se dicta a diario en temas de televisión.

Todos los dominios, objetivos de control y controles que establece la norma son aplicables en cualquier empresa, pero para el caso de INGEPEC LTDA., se seleccionaron sólo los mencionados anteriormente teniendo en cuenta las necesidades de diseñar un Plan de Gestión que establezca los controles para evitar el acceso no autorizado a las áreas seguras, razón por la cual los dominios escogidos son los relacionados con Seguridad Física y Organizativa. No se incluyeron los dominios Gestión de comunicaciones y operaciones, control de acceso y adquisición, desarrollo y mantenimiento de sistemas de información ya que su enfoque es hacia la seguridad lógica y no aplican para el presente trabajo; además la empresa no permitió el acceso a los equipos y datos por ser información confidencial.

## 4.3 ELABORACIÓN DEL PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE UNA SERIE DE LINEAMIENTOS QUE PERMITEN CONTROLAR EL ACCESO A LAS ÁREAS RESTRINGIDAS A LA EMPRESA INGEPEC LTDA.

La información es un activo intangible que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente; esto es especialmente importante en el ambiente comercial cada vez más interconectado, ya que como resultado de esta creciente interconectividad, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades.

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

Conociendo las necesidades en la empresa INGEPEC LTDA. y la importancia de la seguridad de la información en una organización, se formula el documento de Plan de Gestión de Seguridad de la Información que permite establecer los controles necesarios para protegerla y minimizar los riesgos de pérdida de activos o daño en equipos lo cual puede afectar la calidad del servicio ofrecido.

**4.3.1 Documento del plan de gestión de seguridad de la información INGEPEC LTDA.** El objetivo del presente Plan de Gestión de Seguridad de la Información es generar lineamientos que permitan proteger los recursos de almacenamiento de información de la empresa INGEPEC LTDA , y la tecnología utilizada, frente a amenazas internas o externas con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Este documento se dicta en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, el ambiente físico y tecnológico de la empresa INGEPEC LTDA y debe ser conocida y cumplida por todo el personal vinculado a la misma. La definición del periodo de implementación es responsabilidad de las directivas y personal de la empresa.

La implementación, revisión y actualización del Plan de Gestión de Seguridad de la Información es responsabilidad de la Gerencia apoyado en el Comité de Seguridad de la Información de la empresa INGEPEC LTDA, el cual debe crearse de acuerdo a lo establecido en la Política de Seguridad que conforma el presente plan de gestión.

Teniendo en cuenta la presentación dada al documento del plan de gestión de seguridad de la información con diseño de página y formatos especiales que son diferentes al cuerpo del presente trabajo, dicho documento está incluido como anexo Q, aclarando que es el desarrollo del tercer objetivo especifico al que hacemos referencia en el proyecto y en este ítem. Para la elaboración del Plan de Gestión es importante tener en cuenta la asignación de roles y responsabilidades relativas a la seguridad de la información en INGEPEC LTD., por lo tanto, se planteó el siguiente cuadro teniendo en cuenta el personal con que cuenta la empresa y sus funciones frente a la protección de la información.

**Cuadro 12. Asignación de roles y responsabilidades**

| ROL | RESPONSABLE | RESPONSABILIDAD |
|---|---|---|
| Coordinador del Comité de Seguridad de la Información | Gerente | Coordinar las acciones del Comité de Seguridad de la Información.<br>Impulsar la implementación y cumplimiento de la presente Política. |
| Propietarios de la Información | Jefes de área (Comercialización, Distribución y Producción) | Definir que usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. |
| Responsable del Área de Recursos Humanos | Administrador | Notificar a todo el personal que ingrese de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de los procedimientos y prácticas que de ella surjan.<br>Implementar la suscripción de los acuerdos de confidencialidad y las tareas de capacitación en materia de seguridad de la información. |
| Usuarios de la información y los sistemas | Todo el personal | Conocer y cumplir con la Política de Seguridad de la Información. |

**Fuente:** Autores del proyecto

**4.3.2 Propuesta De Implementación Del Plan De Gestión De Seguridad De La Información.** Después de haber diseñado el plan de gestión de seguridad de la información para la empresa INGEPEC LTDA se elaboró adicionalmente una propuesta de posible implementación que puede ser usada por la empresa como herramienta para ello si así lo desea, además se elaboro un presupuesto para que INGEPEC LTDA cuente con una estimación de la inversión que debe realizar para tal fin y estimando el tiempo que se requiere para llevar a cabo dicha implementación tal como se muestra a continuación.

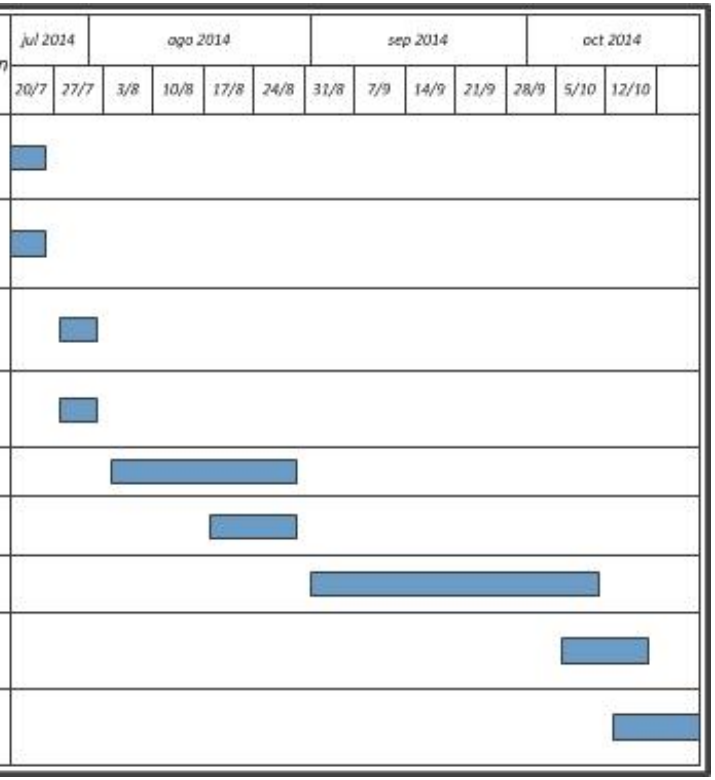
**Cuadro 13.** Propuesta de implementación

| ESTRATEGIAS | RESPONSABLE | RECURSOS EN PESOS |
|---|---|---|
| Definir un comité de gestión de la seguridad de la información que se encargue de la implementación, revisión y actualización de las políticas de seguridad. | GERENTE | $ 0 |
| Definir actividades específicas que ayuden a identificar los requerimientos para la puesta en marcha del plan de gestión de seguridad | COMITÉ DE SEGURIDAD DE LA INFORMACION | $ 200.000 |
| Asignación de cronograma para la realización de las actividades consolidadas y especificadas en la política de seguridad | COMITÉ DE SEGURIDAD DE LA INFORMACION | $ 0 |
| Definición de responsables para la ejecución de cada actividad consolidada como control en la política de seguridad; de acuerdo a las funciones desempeñadas dentro de la empresa. | COMITÉ DE SEGURIDAD DE LA INFORMACION | $ 0 |
| Socialización de la política de seguridad | GERENTE | $ 100.000 |
| Capacitación del personal de la empresa en la nueva estrategia para mejorar la seguridad de la información de INGEPEC LTDA | GERENTE | $ 5.000.000 |
| Puesta en marcha del Plan de Gestión de Seguridad | COMITÉ DE SEGURIDAD DE LA INFORMACION | $ 6.000.000 |
| Implementación de la propuesta de reconocimiento facial para controlar el acceso a áreas restringidas de la empresa | COMITÉ DE SEGURIDAD DE LA INFORMACION | $ 6.000.000 |
| Realización de auditoríasperiódicas por parte del comité de seguridad de la información para evaluar el proceso de implementación del plan de gestión. | COMITÉ DE SEGURIDAD DE LA INFORMACION | $ 0 |
| **TOTAL DE RECURSOS** | | **$ 17.300.000** |

**Fuente**. Autores del proyecto

**Cuadro 14.**Cronograma de implementación

| Id. | Actividades | Comienzo | Fin | Duración |
|---|---|---|---|---|
| 1 | Definir un comité de gestion de la seguridad de la informacion que se encargue de las politicas de seguridad | 21/07/2014 | 25/07/2014 | 1s |
| 2 | Definir actividades específicas que ayuden a identificar los requerimientos para la puesta en marcha del plan | 21/07/2014 | 25/07/2014 | 1s |
| 3 | Asignación de cronograma para la realización de las actividades consolidadas y especificadas en la politica de seguridad | 28/07/2014 | 01/08/2014 | 1s |
| 4 | Definición de responsables para la ejecución de cada actividad consolidada como control en la política de seguridad | 28/07/2014 | 01/08/2014 | 1s |
| 5 | Socialización de la politica de seguridad | 04/08/2014 | 29/08/2014 | 4s |
| 6 | Capacitación del personal de la empresa en la nueva estrategia | 18/08/2014 | 29/08/2014 | 2s |
| 7 | Implementación del plan de gestión de seguridad | 01/09/2014 | 10/10/2014 | 6s |
| 8 | Implementación de la propuesta de reconocimiento facial para controlar el acceso a áreas restringidas | 06/10/2014 | 17/10/2014 | 2s |
| 9 | Ejecución de auditorias periódicas para evaluar el proceso de implementación del plan de gestión. | 13/10/2014 | 24/10/2014 | 2s |




**Fuente**. Autores del proyecto

## 4.4 PROPUESTA ADICIONAL

**Desarrollo de un sistema de reconocimiento biométrico para implementar como control de acceso físico a las áreas de la empresa INGEPEC LTDA.** El reconocimiento biométrico responde a un sistema automático basado en la inteligencia artificial y el reconocimiento de patrones, que permite la identificación y/o verificación de la identidad de personas a partir de características morfológicas o de comportamiento, propias y únicas del individuo, conocidas como autentificadores. Como principales autentificadores podemos mencionar las huellas dactilares, la geometría de la mano, la cara, el termograma facial, el iris, la retina, la voz, el estilo de escritura...etc. Asimismo, la naturaleza del tipo de característica, morfológica o de comportamiento, se encuentra directamente relacionada con el grado de variación de las mismas con el paso del tiempo, siendo mucho más inferior en el primer caso que en segundo, ya que como sabemos, el comportamiento está íntimamente relacionado con factores psicológicos y éstos sí que son función directa del tiempo.

Este tipo de reconocimiento se ha convertido en una herramienta habitual en las fuerzas de la policía durante los procesos de investigación criminal, posibilitando la detención de delincuentes a nivel mundial, aunque también se le reconocen otras aplicaciones específicas tales como el control de acceso a cualquier tipo de transacción o acceso a datos protegidos.

La metodología de implementación básica de un sistema de reconocimiento biométrico está conformada por tres fases:

La fase de entrenamiento o modelado, donde se extraen las características significativas de la señal de entrada, la fase de almacenamiento del modelo obtenido en la fase anterior, y la fase de test, donde se realiza el reconocimiento propiamente dicho. Es evidente la necesidad de una gran base de datos que contenga los patrones necesarios para el tipo de autentificación descrita.

Los sistemas de reconocimiento biométrico de mayor popularidad son: Reconocimiento facial, reconocimiento de huellas dactilares y reconocimiento de iris. La técnica seleccionada para investigación fue la de reconocimiento facial.

**4.4.1 Reconocimiento Facial.** Los seres humanos poseen una alta capacidad para reconocer rostros aún en escenarios donde existan altos niveles de variabilidad. Diseñar sistemas automáticos que emulen esta propiedad natural de los humanos, constituye una tarea compleja y con muchas limitaciones. Probablemente una de las primeras interrogantes sea ¿los rostros son diferenciables como medidas biométricas? Afortunadamente en los últimos años se han realizado una gran cantidad de investigaciones que afirman esta interrogante, en especial el área de la biometría.

**4.4.2 Características de los sistemas de reconocimiento facial.** Características del Autentificador: Responde a una característica de tipo morfológico variable con el tiempo. En particular, la estructura facial responde a dos tipos de cambios temporales: La variación

no agresiva, característica del crecimiento y del envejecimiento del individuo (variación caracterizada por aparecer de forma relativamente lenta), y la variación agresiva, debida principalmente a factores como operaciones de cirugía estética, accidentes, etc, de acción prácticamente inmediata.

**Sistema de Reconocimiento**. Lo sistemas de reconocimiento facial están englobados dentro de las técnicas FRT (FaceRecognitionThecniques). Estas técnicas de aproximación al reconocimiento facial, pueden clasificarse en dos categorías según el tipo de aproximación holística o analítica. La aproximación holística (método de las eigenfaces) considera las propiedades globales del patrón, mientras que la segunda considera un conjunto de características geométricas de la cara. Existen dos divisiones de este segundo tipo de aproximación: la basada en los vectores característicos extraídos del perfil, y la basada en los vectores característicos extraídos a partir de una vista frontal de la cara. El sistema tiene las siguientes características:

Sistema no invasivo (no intrusión física o contacto del autentificador con el sistema de reconocimiento).

Permite la identificación de personas en movimiento.

Sistema con posibilidad de camuflaje (las personas no detectan que son objeto de un proceso de reconocimiento).

Reconocimiento de sujetos no dispuestos a cooperar.

El sistema de captura necesita de una fuente de luz auxiliar.

Susceptible a problemas de iluminación.

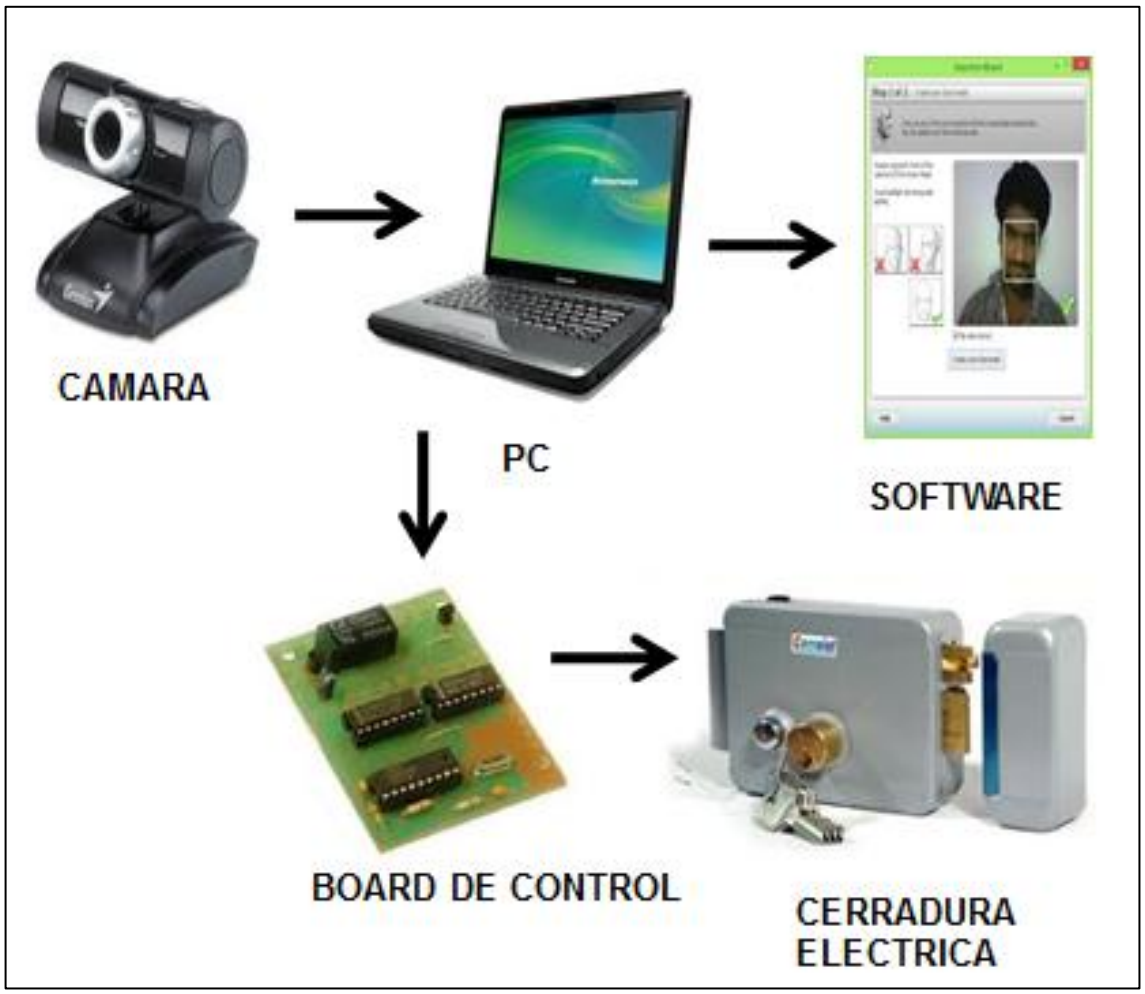
Sistema vulnerable al reconocimiento de sujetos que se han sometido a operaciones de cirugía plástica (estéticas y de cirugía en general).

**4.4.3 I****mplementación de la propuesta.** Actualmente existen librerías gratuitas multiplataforma que ayudan a elaborar programas dedicados a la detección de rostros como Open CV, al igual software de reconocimiento facial de bajo precio como KEYLEMON con el que se implementó el control de acceso para la empresa INGEPEC LTDA , además de este software para realizar la puesta en marcha del sistema se hizo necesario el uso de una cámara web encargada de capturar los rostros, un computador portátil con memoria ram de 2 GB, procesador intelcoreduo, una board de control encargada de decodificar las señales enviadas por el software y proveer la energía necesaria para activar la cerradura eléctrica también usada en esta implementación.

Lo anteriormente mencionado se realizó con el fin de suministrar un control a la empresa INGEPEC LTDA que le permita restringir el acceso a personal no autorizado al cuarto de

equipos tecnológicos de dicha empresa, considerado como el activo más valioso de la organización por contener la información más importante para la misma.

**Figura 12**. Recursos necesarios para la implementación del sistema




**Fuente**. Autores del proyecto

El software Key Lemon está diseñado para iniciar sesiones de Windows mediante reconocimiento facial, dicho software fue modificado para que en el momento de reconocer un rostro que previamente fue grabado en su base de datos envíe información a una tarjeta de control que esta todo el tiempo supervisando la señal enviada por el computador, dicha tarjeta tiene todos los recursos de hardware para activar una cerradura eléctrica que es la que controla el acceso al área restringida de la empresa.

En la base de datos se almacenan los rostros que tienen autorización para ingresar al cuarto de equipos tecnológicos de la empresa, dicho software también registra la hora y la fecha de las personas que fueron autorizadas por el sistema.

# 5. CONCLUSIONES

Mediante el desarrollo de actividades como la aplicación de un estudio a los empleados, el análisis a la gestión de activos, la caracterización de la información y la aplicación de una matriz de riesgos en la organización; se logró establecer criterios claros para dar cumplimiento al diagnostico del estado actual de la seguridad física y ambiental determinando que existen falencias y vulnerabilidades que ponen en riesgo la seguridad de la información y que comprometen la confidencialidad, integridad y disponibilidad de la misma. Por su parte la realización de la auditoria a la seguridad física y del entorno permitió diagnosticar que la empresa se encuentra estructural y administrativamente bien organizada, sin embargo no cuenta con controles de seguridad definidos para evitar el acceso físico no autorizado; todas estas falencias son consecuencia de no planear ni implementar políticas de seguridad que orienten a la organización para la aplicación de buenas prácticas en la gestión de la información.

Después de identificar y analizar los componentes que integran el plan de gestión de seguridad de la información de acuerdo a las normas ISO 27001 Y 27002 y teniendo en cuenta las necesidades de la empresa; se estableció trabajar en el plan de gestión de seguridad ocho dominios como son, política de seguridad, organización de la seguridad de la información, gestión de activos, seguridad ligada a los recursos humanos, seguridad física y del entorno, gestión de incidentes en la seguridad de la información, gestión de la continuidad del negocio y cumplimiento; de igual manera se incluyeron elementos que complementan y orientan la implementación de las políticas de seguridad establecidas en el plan, estos elementos son: un objetivo general, un alcance, definición de responsables, recursos, estrategias y actividades para la implementación.

Se elaboró el Plan de Gestión de Seguridad de la Información como documento que establece los lineamientos para proteger los recursos de almacenamiento de información y la tecnología utilizada de la empresa INGEPEC LTDA frente a amenazas internas o externas, con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información. Como apoyo al Plan de Gestión se diseñó una propuesta adicional que permite incentivar a la empresa para que implemente controles adecuados que le ayuden a mejorar la seguridad de la información; el aporte consistió en el desarrollo de un sistema biométrico que permite controlar el acceso físico no autorizado; dicha propuesta se realizó mediante el uso de un software de reconocimiento facial de bajo precio llamado KEYLEMON, además el uso de una cámara web encargada de capturar los rostros, un computador portátil con memoria RAM de 2 GB, procesador intel core duo, una board de control encargada de decodificar las señales enviadas por el software y proveer la energía necesaria para activar la cerradura eléctrica también usada en esta implementación.

# 6. RECOMENDACIONES

Se recomienda a la Gerencia de INGEPEC LTDA aprobar e implementar el Plan de Gestión de Seguridad de la Información y comunicarlo a todo el personal vinculado a la empresa con el fin de garantizar el cumplimiento y efectividad de los controles establecidos para mantener la confidencialidad, integridad y disponibilidad de la información. De igual manera se sugiere tener en cuenta la propuesta de implementación planteada en este proyecto como guía para que la empresa se oriente en las estrategias, tiempo y recursos financieros necesarios para la puesta en marcha del Plan de Gestión.

Con el objeto de hacer seguimiento y control a las políticas de seguridad formuladas en el Plan de Gestión y verificar su efectividad, se recomienda realizar auditorías periódicas que permitan evaluar y mejorar los controles propuestos, teniendo en cuenta los instrumentos de recolección de información y análisis de datos planteados en la auditoría realizada por el equipo de trabajo del proyecto. De esta manera se busca garantizar que la empresa INGEPEC LTDA., contraataque las interrupciones a las actividades comerciales y proteja los procesos que puedan afectar las operaciones esenciales mediante la seguridad de la información como parte integral del proceso gerencial asegurando la continuidad del negocio.

Por último, se recomienda el uso del sistema biométrico de reconocimiento facial diseñado en el presente proyecto para controlar el acceso físico no autorizado a las áreas seguras de INGEPEC LTDA., teniendo en cuenta que es un control tecnológico efectivo e innovador que le permite a la empresa iniciar con la cultura de seguridad de la información y que su implementación resulta viable económicamente.

## BIBLIOGRAFIA

REPÚBLICA DE COLOMBIA, Constitución Política De La República De Colombia De 1991, Actualizada hasta el Decreto 2576 del 27 de Julio de 2005

Norma ISO/IEC 27002:2005

AGUILERA LOPEZ, Purificacion. Seguridad informática. Tercera edición. Editorial casa del libro. 2010. p. 125.

SANCHEZ CALLE, Angel. Aplicaciones de la visión artificial y la biometría informática. Universidad Rey Juan Carlos

## REFERENCIAS DOCUMENTALES ELECTRONICAS


SISTESEG. [En línea Disponible desde Internet en: <http://www.sisteseg.com/> [con acceso el 06-12-2013]

POLITICA DE SEGURIDAD FÍSICA. SISTESEG. [En línea]. Disponible desde Internet en: <http://www.sisteseg.com/files/Microsoft_Word_-_Politica_Seguridad_Fisica.pdf>[con acceso el 06-12-2013]

CENTRO NACIONAL DE INTELIGENCIA, Autoridad Nacional para la protección de la información clasificada, Norma NS/03, Edición 2.0 Diciembre 2012. [En línea Disponible desde Internet en:http://www.cni.es/comun/recursos/descargas/NS-03_Seguridad_Fisica.pdf[con acceso el 06-12-2013]

CONGRESO DE LA REPUBLICA COLOMBIANA. LEY 1273 DE 2009 (enero 5). [En línea]. Disponible desde Internet en: <http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html> [con acceso el 07-12-2013]

DUSSAN CLAVIJO, Ciro Antonio; 2006 (Enero - Junio). Políticas de seguridad informática. Vol.2 No. 1 [En línea]. Disponible desde Internet en: <http://www.unilibrecali.edu.co/entramado/images/stories/pdf_articulos/volumen2/Politicas_de_seguridad_informtica.pdf>[con acceso el 08-12-2013]

LA TEORÍA GENERAL DE LA INFORMACIÓN, UNA CIENCIA MATRIZ. [En línea]. Disponible desde Internet en: <http://www.infoamerica.org/teoria_articulos/benito01.pdf> [con acceso el 08-12-2013]

# ANEXOS

**Anexo A.** Encuesta dirigida a personal de la empresa INGEPEC LTDA

**Objetivo:** Recolectar información para conocer la necesidad de diseñar el plan de gestión de seguridad para controlar el acceso a las áreas restringidas de la empresa INGEPEC LTDA .

**NOMBRE DEL EMPLEADO _____ CARGO_____**

1. ¿Existe en la empresa un plan de gestión de seguridad?

SI ____ NO _____

2. ¿Utiliza perímetros de seguridad para proteger las áreas que contienen información y medios de procesamiento de la misma?.

SI ____ NO _____

3. ¿Las áreas seguras se encuentran protegidas mediante controles de ingreso apropiados para asegurar que solo se le permita el acceso a personal autorizado?

SI ____ NO _____

4. ¿Cuáles mecanismos para el control de acceso utiliza la empresa?

Sistemas Biométricos ____ Medios Físicos _____ Otros

5. ¿Están definidos los lineamientos para trabajar en áreas aseguradas?

SI____ NO_____

6.¿ Existen métodos de protección de los equipos que permitan reducir el riesgo de acceso no autorizado a la información y protegerla contra perdida o daño?

SI_____NO_____

**¡Muchas gracias por su tiempo!**

**Anexo B.** Lista de chequeo conocimientos de seguridad de la información en la empresa INGEPEC LTDA.

| | | | | |
|---|---|---|---|---|
| **COANCO Auditores Ltda.** | | | | |
| **Objetivo:** Indagar sobre las políticas y normas de seguridad de la empresa INGEPEC LTDA | | | | |
| **LISTA DE NORMAS ISO/IEC 27001 - 27002** | | **SI** | **NO** | **OBSERVACION** |
| **Conceptos básicos** | | | | |
| 1 | Conoce que es seguridad de la información | ✓ | | |
| 2 | Tiene un concepto de lo que son áreas restringidas | ✓ | | |
| 3 | Sabe que es un riesgo | ✓ | | |
| 4 | Identifica que es control de acceso físico | ✓ | | |
| **Conocimiento normativo y aplicabilidad** | | | | |
| 5 | Su empresa ha adquirido alguna norma que se refiera a seguridad de la información | | X | No se ha preocupado por este aspecto porque no se conoce la importancia. |
| 6 | Existe un plan de gestión establecido para controlar la seguridad de la información y de los activos de la empresa. | | X | No se conoce los beneficios de un plan de gestión de seguridad |
| 7 | Se cuenta con una política de seguridad establecida | | X | No se ha recibido asesoría de este tema |
| 8 | La empresa tiene reglamento para el acceso físico a la empresa | ✓ | | Existe reglamento interno donde se establece el área de acceso restringido, política de mantener las puertas cerradas y |
| 9 | A consultado la norma ISO 271001 | | X | No se conoce |
| 10 | Tiene conocimiento de que es un riesgo | ✓ | | |
| 11 | Sabe cómo aplicar controles de seguridad | | X | |
| 12 | Le gustaría que en su empresa existiera un plan de gestión de seguridad. | ✓ | | |
| 13 | Utiliza mecanismos para el control de acceso | ✓ | | Puertas, cerraduras y candados |

**Anexo C.** Programa de Auditoria

**CO Auditores Ltda.**

| PROGRAMA DE AUDITORIA | |
|---|---|
| **EMPRESA AUDITADA:** INGEPEC LTDA. | **FECHA: 15 DE ENERO DE 2014** |
| **REPRESENTANTE LEGAL:** RAUL ROCHEL OJEDA | |
| **AREA:** EMPRESA | |

**OBJETIVO GENERAL**: Evaluar la seguridad física y ambiental de la empresa INGEPEC LTDA .

**OBJETIVOS ESPECÍFICOS:**

**1.** Revisar el perímetro de seguridad física de la empresa INGEPEC LTDA .

**2.** Verificar los controles de ingreso físico a las áreas de acceso restringido.

**3.** Examinar la seguridad del cableado de la energía y las telecomunicaciones.

**ALCANCE:** La presente auditoria se realizará a la empresa INGEPEC LTDA ., ubicada en Ocaña Norte de Santander en la calle 10 N° 11-29 San Agustín, en un periodo de un mes comprendido entre el 20 de Enero hasta el 20 de Febrero de 2014.

| FASE | ACTIVIDAD | DESCRIPCION | N° DE PERSONAL PARTICIPANTE | PERIODO ESTIMADO | | DIAS HABILES |
|---|---|---|---|---|---|---|
| | | | | INICIO | FINAL | |
| **Visita Preliminar** | Se realiza una visita al sitio que será auditado para realizar el reconocimiento y hacer la presentación formal con el personal a auditar. | Presentación del personal a auditar y del equipo auditor.<br><br>Reconocimiento de las instalaciones de la empresa INGEPEC LTDA . | Gerente y Equipo Auditor | 20/01/14 | 20/01/14 | 1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Objetivo 1** | Visita a todas las áreas de la empresa INGEPEC LTDA . | Utilizar la observación directa para identificar los controles de seguridad física existentes, verificar su efectividad y diligenciar el formato de situaciones. | 1 Integrante del equipo Auditor | 21/01/14 | 22/01/14 | 2 |
| | Realización de entrevista | La entrevista se aplicará a dos empleados de la empresa con el fin de indagar sobre la seguridad física de cada área. | 1 Integrante del equipo Auditor 2 empleados de la empresa INGEPEC LTDA . | 23/01/14 | 24/01/14 | 2 |
| **Objetivo 2** | Revisar la actualización de la bitácora | Solicitud de la bitácora para observar los datos que contiene la misma y verificar su actualización. | 1 Integrante del equipo Auditor 1 empleado encargado de llevar la bitácora | 25/01/14 | 26/01/14 | 2 |
| | Realización de entrevista | La entrevista se realizará al gerente de la empresa INGEPEC LTDA ., con el fin de identificar la existencia de herramientas y dispositivos de control y seguridad de acceso a las áreas | 1 Integrante del equipo Auditor El gerente de la empresa | 27/01/14 | 28/01/14 | 2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | restringidas. | | | | |
| **Objetivo 3** | Realización de entrevista | La entrevista se realizará al Técnico en Mantenimiento para verificar si existe sistema de codificación de control de usuarios, con el fin de determinar los controles aplicados por la empresa para evitar el robo de señal. | 1 Integrante del equipo Auditor El Técnico en Mantenimiento | 29/01/14 | 30/01/14 | 2 |
| | Realizar visita a la cabecera de red de televisión por cable y aplicar una lista de chequeo. | Por medio de la observación directa se identificará la existencia de decodificadores y al aplicar la lista de chequeo al Técnico en Mantenimiento se determinará la sensibilidad del sistema. | 2 Integrantes del equipo Auditor El Técnico en Mantenimiento | 1/02/14 | 2/02/14 | 2 |
| | Inspección de los tendidos de cableados de energía y telecomunicaciones. | A través de una visita al área de producción, realizar la inspección a los tendidos de cableado para determinar los controles de | 1 Integrante del equipo Auditor | 3/02/14 | 4/02/14 | 2 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | protección contra intercepción o daño. | | | | |
| **Revisión y pre-informe** | Una vez recolectada toda la información por medio de entrevista, observaciones se comienza con la elaboración y revisión de toda la documentación necesaria para realizar el informe final. | Revisión de los papeles de trabajo. Diagnóstico. Elaboración del oficio de presentación. Elaboración del borrador. | Equipo Auditor | 5/02/14 | 17/02/14 | 13 |
| **Dictamen** | Elaboración y presentación del dictamen. | Presentación del dictamen al Gerente de la empresa INGEPEC LTDA., comunicación de resultados por parte del Auditor Líder. | Gerente y Auditor Líder | 18/02/14 | 20/02/14 | 3 |
| **ELABORÓ:** EQUIPO AUDITOR | | | **APROBÓ:** EQUIPO AUDITOR | | | |

**Anexo D.**Guía de Auditoria

| COANCO Auditores Ltda. | | | | |
|---|---|---|---|---|
| **GUIA DE AUDITORIA** | | | | |
| **EMPRESA: INGEPEC LTDA** | | | **DIA** | **MES** / **AÑO** |
| | | | 18 | 01 / 2014 |
| **REFERENCIA** | **ACTIVIDAD O FUNCION A EVALUAR** | **PROCEDIMIENTO** | **HERRAMIENTAS** | **OBSERVACION** |
| GA.01 | Evaluar la seguridad física y ambiental de la empresa INGEPEC LTDA . | Realización de visita a las instalaciones para observar la características físicas y ambientales de la empresa INGEPEC LTDA y de esta manera realizar una evaluación a las mismas | Observación<br><br>Pruebas<br><br>Revisión documental<br><br>Diligenciamiento de situaciones encontradas en formatos diseñados previamente | Debe existir un perímetro de seguridad donde se encuentren resguardados los equipos de producción.<br><br>Debe haber un empleado de la empresa que tenga establecidas las funciones del control de acceso a los perímetros restringidos.<br><br>Las cerraduras de puertas y ventanas debe ser el adecuado teniendo en cuenta la norma ISO 170001 |

| | | | | |
|---|---|---|---|---|
| GA. 02 | Verificar los controles de ingreso físico a las áreas de acceso restringido. | Ingresar a las áreas donde se encuentran los equipos de redes y tomar evidencia de los procedimientos y solicitudes realizadas por la empresa para el ingreso de empleados y particulares | Pruebas<br><br>Observación<br><br>entrevista abierta con los empleados | Al realizar la solicitud de ingreso a las áreas de producción, donde reposan los equipos y la información de la empresa, debe existir aparatos electrónicos que registren el ingreso al lugar, de igual manera debe quedar un registro físico y dactilar. |
| GA.03 | Examinar la seguridad del cableado de la energía y las telecomunicaciones | Solicitar una terminal para ingresar a la cabecera y acceder a los decodificadores del sistema de televisión y observar los permisos otorgados a los usuarios para acceder a la señal | Pruebas<br><br>Observación<br><br>entrevista abierta con los empleados<br><br>reportes tomados de los decodificadores | Al ingresar a los decodificadores e intentar acceder a ver la señal de usuarios que tienen suspendido el sistema no debe estar activada y al realizar reconexiones al sistema de manera inmediata debe activarse la señal. |
| **ELABORÓ:** EQUIPO AUDITOR | | **APROBÓ:** EQUIPO AUDITOR | | |

**Anexo E.**Formato situaciones encontradas evaluando los controles de seguridad física existentes y su efectividad**.**

**COAN Auditores Ltda.**

**FORMATO SITUACIONES ENCONTRADAS**
**VISITA DE OBSERVACION**

| **EMPRESA** | **DIA** | **MES** | **AÑO** |
|---|---|---|---|
| INGEPEC LTDA . | 20 | 01 | 2014 |

**OBJETIVO 1:** Revisar el perímetro de seguridad física de la empresa INGEPEC LTDA .

| **AREA AUDITADA** | **SITUACIONES ENCONTRADAS** | **CAUSAS** | **RECOMENDACIONES** | **RESPONSABLE** |
|---|---|---|---|---|
| **PRODUCCIÓN** | No existen perímetros de seguridad definidos en la cabecera de red que protejan el área, se conoce por parte del personal de la empresa que a esta área solo ingresa personal autorizado en este caso el Técnico en mantenimiento, los operarios y el gerente.<br><br>Las cerraduras de las puertas no son seguras, lo que origina que cualquier persona pueda manipular los equipos y acceder a la información procesada en el área. | No existen controles de entrada apropiados.<br><br>No existen un empleado que vigile el ingreso a esta área<br><br>Las puertas para el ingreso al área no tienen mecanismos de control de seguridad.<br><br>El área donde se encuentran instalados los equipos de transmisión de señal no cuenta con la política de acceso | Definir los perímetros de seguridad para evitar el acceso físico no autorizado, las puertas deben estar protegidas contra accesos no autorizados mediante mecanismos de control como cerradura electrónica, control de ingreso con identificación dactilar, además deben quedar aseguradas cuando no haya personal dentro del área, con el fin de proveer protección al área y evitar daño e interferencia en la información. | Gerente |

| | | | | |
|---|---|---|---|---|
| | | restringido. | | |
| **COMERCIALIZACION** | Deficiencia en la seguridad física para ingresar al área de servicio al cliente en la cual se reciben pagos en efectivo. | No existen barreras blindadas que aseguren el área de servicio al cliente, ni se cuenta con personal de vigilancia privada. | Implementar barreras físicas como vidrio blindado en el área de servicio al cliente y contratar personal de vigilancia privada que permita controlar el acceso físico, restringiendo el acceso solo a personal autorizado. | Gerente |
| **Elaboró:**<br>**Esp. María Liliana Suarez Domínguez** | | **Aprobó:**<br>**Esp. Liseth Tatiana Angarita López** | | |

**Anexo F.**Entrevista para evaluar la seguridad física de cada área de la empresa INGEPEC LTDA .

| **COANCO Auditores Ltda.** | | | |
|---|---|---|---|
| **FORMATO DE ENTREVISTA** | | | |
| **EMPRESA** | **DIA** | **MES** | **AÑO** |
| INGEPEC LTDA . | 21 | 01 | 2014 |
| **ENTREVISTADO:** SAID ARIAS BARBOSA | | | |
| **CARGO:** Técnico en Mantenimiento | | | |
| **OBJETIVO 1:** Revisar el perímetro de seguridad física de la empresa INGEPEC LTDA . | | | |
| **1.** ¿Cómo detecta usted que a las áreas de acceso restringido ingresa solo el personal autorizado y cuáles son los mecanismos de control? | | | |
| **2.** ¿Si una persona no autorizada para ingresar al área de producción manipula los equipos y causa daño en la información, como controla usted esta situación? | | | |
| **3.** ¿Se evidencia que no existe perímetros de seguridad en el área, por lo tanto si ocurre pérdida o daño de la información quien es el responsable? | | | |
| **4.** ¿Cuáles razones considera usted que existen para que los administrativos de la empresa no establezcan controles eficaces para el ingreso al área de producción? | | | |
| **5.** Describa cuales son los controles de seguridad física que usted como encargado del área utiliza y cuál es la efectividad de los mismos. | | | |
| **ELABORÓ:** EQUIPO AUDITOR | **APROBÓ:** EQUIPO AUDITOR | | |

**Anexo G.**Prueba de cumplimiento. Políticas de Seguridad

| **COANCO Auditores Ltda.** | |
|---|---|
| **INGEPEC LTDA .** | |
| **PRUEBA** | Políticas de seguridad |
| **OBJETIVO** | Revisar el perímetro de seguridad física de la empresa INGEPEC LTDA . |
| **TÉCNICA** | Observación<br>Entrevista |
| **TIPO DE PRUEBA** | Cumplimiento |
| **PROCEDIMIENTO A EMPLEAR** | 1. Solicitar el documento marco de las políticas de seguridad donde se identifiquen cuáles son las áreas establecidas como acceso restringido.<br>2. Verificar si lo que establece el documento se cumple. |
| **RECURSOS** | Documental<br>Humanos |
| **RESULTADOS DE LA PRUEBA** | |
| **HALLAZGOS** | Se encuentra diseñado el documento de políticas de seguridad donde se señalan las áreas restringidas, sin embargo se presentan las siguientes situaciones relevantes:<br><br>No existen perímetros de seguridad física.<br><br>No existen controles de entrada apropiados.<br><br>No existe un empleado que vigile el ingreso al área de producción.<br><br>Las puertas para el ingreso a las áreas de la empresa no tienen mecanismos de control de seguridad.<br><br>El área de producción en donde se encuentran instalados los equipos de transmisión de señal no cuenta con la política de acceso restringido. |
| **CAUSAS** | La empresa no tiene establecido controles para el cumplimiento de las políticas de seguridad |

| | |
|---|---|
| | establecidas. |
| **SITUACIÓN DE RIESGO QUE GENERA** | Vulnerabilidad de la información<br>Pérdida de la información<br>Pérdida de activos<br>Daño de equipos |
| **RECOMENDACIONES DE AUDITORIA** | Definir los perímetros de seguridad para evitar el acceso físico no autorizado, las puertas deben estar protegidas contra accesos no autorizados mediante mecanismos de control como cerradura electrónica, control de ingreso con identificación dactilar, además deben quedar aseguradas cuando no haya personal dentro del área, con el fin de proveer protección al área y evitar daño e interferencia en la información. |
| **FECHA** | 10 de Febrero de 2014 |
| **ELABORADO POR: Esp. Maria Liliana Suarez Dominguez** | |
| **REVISADO POR: Esp. Liseth Tatiana Angarita López** | |

**Anexo H.**Formato de situaciones encontradas de la revisión de la bitácora.

| | | | | |
|---|---|---|---|---|
| **COANCO Auditores Ltda.** | | | | |
| **FORMATO SITUACIONES ENCONTRADAS<br>VISITA DE OBSERVACION** | | | | |
| **EMPRESA** | | **DIA** | **MES** | **AÑO** |
| INGEPEC LTDA . | | 22 | 01 | 2014 |
| **OBJETIVO 2:** Verificar los controles de ingreso físico a las áreas de acceso restringido. | | | | |
| **AREA AUDITADA** | **SITUACIONES ENCONTRADAS** | **CAUSAS** | **RECOMENDACIONES** | **RESPONSABLE** |
| **PRODUCCIÓN** | Sí existe la bitácora como control de acceso al área de producción, contiene datos de la persona que ingresa nombre, cargo, fecha, hora de entrada, hora de salida y observación. Sin embargo al revisarla se observa que la última entrada al área fue el día 26 de Julio del año 2013 y el día 8 de Mayo del mismo año se encuentran registrados datos de una persona que no pertenece a la empresa y no se dejó observación sobre el motivo de este ingreso. | No se actualiza la bitácora.<br><br>No existe control de acceso físico al área. | Mantener actualizada la bitácora registrando todos los días la información del personal que ingresa al área, con el fin que el control sea efectivo.<br><br>Cuando ingrese personal no autorizado se debe dejar constancia de la autorización por parte del Gerente. | Técnico en Mantenimiento |
| **Elaboró:<br>Esp. María Liliana Suarez Domínguez** | | **Aprobó:<br>Esp. Liseth Tatiana Angarita López** | | |

**Anexo I.**Entrevista para identificar la existencia de herramientas y dispositivos de control de seguridad para el acceso a las áreas restringidas.

| **COANCO Auditores Ltda.** | | | |
|---|---|---|---|
| **FORMATO DE ENTREVISTA** | | | |
| **EMPRESA** | **DIA** | **MES** | **AÑO** |
| INGEPEC LTDA . | 22 | 01 | 2014 |
| **ENTREVITADO:** RAUL ROCHEL OJEDA | | | |
| **CARGO:** Gerente | | | |
| **OBJETIVO 2:** Verificar los controles de ingreso físico a las áreas de acceso restringido. | | | |
| **1.** ¿Existen claramente definidos los controles de ingreso físico para el acceso a las áreas restringidas, menciónelos? | | | |
| **2.** ¿Por qué la empresa dentro de su política de seguridad no cuenta con personal de vigilancia privada? | | | |
| **3.** ¿De qué manera evalúa usted la efectividad de los controles que existen en la empresa? | | | |
| **4.** ¿Qué situaciones se han presentado para que usted autorice el ingreso de personal externo al área de producción? | | | |
| **5.** ¿Cómo supervisa usted desde la Gerencia que los controles que existen se están cumpliendo correctamente? | | | |
| **ELABORÓ:** EQUIPO AUDITOR | **APROBÓ:** EQUIPO AUDITOR | | |

**Anexo J.**Prueba de cumplimiento. Control de acceso

| **COANCO Auditores Ltda.** | |
|---|---|
| **INGEPEC LTDA .** | |
| **PRUEBA** | Control de acceso |
| **OBJETIVO** | Verificar los controles de ingreso físico a las áreas de acceso restringido. |
| **TÉCNICA** | Observación<br>Entrevista |
| **TIPO DE PRUEBA** | Cumplimiento |
| **PROCEDIMIENTO A EMPLEAR** | 1. Solicitar la autorización para ingresar a las áreas de acceso restringido.<br>2. Identificar los dispositivos y las herramientas de control y seguridad de acceso. |
| **RECURSOS** | Humanos |
| **RESULTADOS DE LA PRUEBA** | |
| **HALLAZGOS** | No existen herramientas electrónicas que registren los accesos a las áreas restringidas.<br>Existe la bitácora como control de acceso manual para registrar el personal que ingresa al área de producción pero no se actualiza. |
| **CAUSAS** | La empresa no ha establecido los dispositivos ni herramienta que permitan control de acceso a áreas restringidas. |
| **SITUACIÓN DE RIESGO QUE GENERA** | Pérdida de activos.<br>Vulnerabilidad de la información.<br>En caso de eventos ocurridos en las áreas restringidas no se puede identificar el o los responsables.<br>Fallas en la prestación del servicio de televisión. |
| **RECOMENDACIONES DE AUDITORIA** | Adquirir herramientas tecnológicas de control de acceso que permitan clasificar e identificar el personal que ingresa a las áreas y que manipulan los equipos. |
| **FECHA** | 11 de Febrero de 2014 |
| **ELABORADO POR: Esp. Maria Liliana Suarez Dominguez** | |
| **REVISADO POR: Esp. Liseth Tatiana Angarita López** | |

**Anexo K.**Prueba de cumplimiento. Revisión de la bitácora

| **COANCO Auditores Ltda.** | |
|---|---|
| **INGEPEC LTDA .** | |
| **PRUEBA** | Revisión de la bitácora |
| **OBJETIVO** | Verificar los controles de ingreso físico a las áreas de acceso restringido. |
| **TÉCNICA** | Observación<br>Revisión documental |
| **TIPO DE PRUEBA** | Sustantiva |
| **PROCEDIMIENTO A EMPLEAR** | 1. Solicitar copia de la bitácora<br>2. Solicitar autorización para ingresar al área de producción. |
| **RECURSOS** | Humanos<br>Documental |
| **RESULTADOS DE LA PRUEBA** | |
| **HALLAZGOS** | Sí existe la bitácora como control de acceso al área de producción, contiene datos de la persona que ingresa nombre, cargo, fecha, hora de entrada, hora de salida y observación. Sin embargo al revisarla se observa que la última entrada al área fue el día 26 de Julio del año 2013 y el día 8 de Mayo del mismo año se encuentran registrados datos de una persona que no pertenece a la empresa y no se dejó observación sobre el motivo de este ingreso. |
| **CAUSAS** | No se actualiza la bitácora.<br><br>No existe control de acceso físico al área. |
| **SITUACIÓN DE RIESGO QUE GENERA** | Pérdida de la información<br><br>Alteraciones en la prestación del servicio de televisión<br><br>Daño en los equipos. |
| **RECOMENDACIONES DE AUDITORIA** | Mantener actualizada la bitácora registrando todos los días la información del personal que ingresa al área, con el fin que el control sea efectivo.<br><br>Cuando ingrese personal no autorizado se debe dejar constancia de la autorización por parte del Gerente. |
| **FECHA** | 14 de Febrero de 2014 |
| **ELABORADO POR: Esp. Maria Liliana Suarez Dominguez** | |
| **REVISADO POR: Esp. Liseth Tatiana Angarita López** | |

**Anexo L.**Entrevista para determinar los controles aplicados por la empresa para evitar el robo de señal

| **COANCO Auditores Ltda.** | | | |
|---|---|---|---|
| **FORMATO DE ENTREVISTA** | | | |
| **EMPRESA** | **DIA** | **MES** | **AÑO** |
| INGEPEC LTDA . | 23 | 01 | 2014 |
| **ENTREVITADO:** SAID ARIAS BARBOSA | | | |
| **CARGO:** Técnico en Mantenimiento | | | |
| **OBJETIVO 3:** Examinar la seguridad del cableado de la energía y las telecomunicaciones. | | | |
| **1.** ¿Existen mecanismos en la empresa para evitar que usuarios no autorizados accedan al servicio? | | | |
| **2.** ¿Cuáles de los siguientes mecanismos tienen implementados para evitar el acceso al servicio: sistemas codificados, trampas o candados de radiofrecuencia? | | | |
| **3.** ¿Realizan supervisiones permanentes al sistema para verificar los usuarios no autorizados instalados en la red? | | | |
| **4.** ¿Los dispositivos de conexión al usuario existentes están protegidos mediante cajas de seguridad? | | | |
| **5.** ¿Existe un sistema de codificación para la totalidad de los canales que le ofrecen al usuario, describa como se cumple con este control? | | | |
| **ELABORÓ:** EQUIPO AUDITOR | **APROBÓ:** EQUIPO AUDITOR | | |

**Anexo M.**Formato de situaciones encontradas al examinar la seguridad del cableado de la energía y las telecomunicaciones

| | | | | |
|---|---|---|---|---|
| **COANCO Auditores Ltda.** | | | | |
| **FORMATO SITUACIONES ENCONTRADAS<br>VISITA DE OBSERVACION** | | | | |
| **EMPRESA** | | **DIA** | **MES** | **AÑO** |
| INGEPEC LTDA . | | 25 | 01 | 2014 |
| **OBJETIVO 3:** Examinar la seguridad del cableado de la energía y las telecomunicaciones. | | | | |
| **AREA AUDITADA** | **SITUACIONES ENCONTRADAS** | **CAUSAS** | **RECOMENDACIONES** | **RESPONSABLE** |
| **PRODUCCIÓN** | Los tendidos de cable no cuentan con etiquetado que permita su fácil identificación.<br><br>No existe protección en los tendidos de cable mediante parrillas o canaletas.<br><br>Los cableados de distribución se encuentran a la vista lo que facilita su intercepción. | No hubo planeación en el momento de realizar el tendido del cableado. | El cableado de la red debe estar protegido contra intercepciones no autorizadas o daños, por ejemplo, utilizando un tubo o evitando las rutas a través de áreas públicas.<br><br>Se deben utilizar marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados. | Técnico en Mantenimiento<br><br>Gerente |
| **Elaboró:<br>Esp. María Liliana Suarez Dominguez** | | **Aprobó:<br>Esp. Liseth Tatiana Angarita López** | | |

**Anexo N.**Lista de Chequeo para examinar la seguridad del cableado

| **COANCO Auditores Ltda.** | | | |
|---|---|---|---|
| **LISTA DE CHEQUEO** | | | |
| **EMPRESA: INGEPEC LTDA** | **DIA** | **MES** | **AÑO** |
| **OBJETIVO 3:** Examinar la seguridad del cableado de la energía y las telecomunicaciones | 25 | 01 | 2014 |
| **CRITERIO DE CUMPLIMIENTO** | **CUMPLE** | | |
| ¿El cableado de energía y telecomunicaciones que van a los medios de procesamiento de información están sujetos con protección adecuada? | **X** | | |
| ¿El cableado de la red está protegido contra intercepciones no autorizadas o daños? | **X** | | |
| ¿El cableado está debidamente marcado? | **X** | | |
| ¿El cableado está protegido mediante parrillas o canaletas? | **X** | | |
| ¿Los equipos son claramente identificables para minimizar errores en la manipulación? | ✓ | | |
| ¿Los cables de energía están separados de los cables de comunicaciones para evitar la interferencia? | ✓ | | |
| ¿Los dispositivos de conexión al usuario están protegidos mediante cajas de seguridad? | **X** | | |
| ¿Existen mecanismos en la empresa para evitar que usuarios no autorizados manipulen el cableado y accedan a la señal? | **X** | | |
| **ELABORÓ:** EQUIPO AUDITOR | **APROBÓ:** EQUIPO AUDITOR | | |

**Anexo O.**Prueba de cumplimiento. Seguridad del cableado

| **COANCO Auditores Ltda.** | |
|---|---|
| **INGEPEC LTDA .** | |
| **PRUEBA** | Seguridad del cableado |
| **OBJETIVO** | Examinar la seguridad del cableado de la energía y las telecomunicaciones. |
| **TÉCNICA** | Observación<br>Entrevista<br>Lista de chequeo |
| **TIPO DE PRUEBA** | Cumplimiento |
| **PROCEDIMIENTO A EMPLEAR** | 1. Solicitar una terminal para ingresar a la cabecera y acceder a los decodificadores del sistema de televisión y observar los permisos otorgados a los usuarios para acceder a la señal. |
| **RECURSOS** | Humanos<br>Cámaras fotográficas |
| **RESULTADOS DE LA PRUEBA** | |
| **HALLAZGOS** | Los tendidos de cable no cuentan con etiquetado que permita su fácil identificación.<br><br>No existe protección en los tendidos de cable mediante parrillas o canaletas.<br><br>Los cableados de distribución se encuentran a la vista lo que facilita su intercepción. |
| **CAUSAS** | No hubo planeación en el momento de realizar el tendido del cableado. |
| **SITUACIÓN DE RIESGO QUE GENERA** | Interferencia en la prestación del servicio.<br>Pérdida de señal |
| **RECOMENDACIONES DE AUDITORIA** | El cableado de la red debe estar protegido contra intercepciones no autorizadas o daños, por ejemplo, utilizando un tubo o evitando las rutas a través de áreas públicas.<br><br>Se deben utilizar marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados. |
| **FECHA** | 12 de Febrero de 2014 |
| **ELABORADO POR: Esp. Hulber Rodrigo Rodríguez Pinzón** | |
| **REVISADO POR: Esp. Liseth Tatiana Angarita López** | |

**Anexo P.**Prueba sustantiva. Informe fotográfico de la terminal del cableado

| **COANCO Auditores Ltda.** | |
|---|---|
| **INGEPEC LTDA .** | |
| **PRUEBA** | Informe fotográfico de la terminal del cableado. |
| **OBJETIVO** | Examinar la seguridad del cableado de la energía y las telecomunicaciones. |
| **TÉCNICA** | Observación |
| **TIPO DE PRUEBA** | Sustantiva |
| **PROCEDIMIENTO A EMPLEAR** | 1. Verificar la existencia de marcas en el cableado mediante la observación y evidencias fotográficas. |
| **RECURSOS** | Humanos<br>Digitales |
| **RESULTADOS DE LA PRUEBA** | |
| **HALLAZGOS** | El cableado no está marcado lo que genera inconvenientes en la identificación de energía y datos. |
| **CAUSAS** | No existió planeación al realizar el tendido del cableado. |
| **SITUACIÓN DE RIESGO QUE GENERA** | Interferencia de señal<br><br>Conflicto en la realización de mantenimientos<br><br>Pérdida de señal |
| **RECOMENDACIONES DE AUDITORIA** | Se deben utilizar marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados. |
| **FECHA** | 15 de Febrero de 2014 |
| **ELABORADO POR: Esp. Hulber Rodrigo Rodríguez Pinzón** | |
| **REVISADO POR: Esp. Liseth Tatiana Angarita López** | |