

## RESUMEN ANALITICO DE INVESTIGACIÓN

-RAI-

### IMPLEMENTACIÓN EN LA FASE DE PLANEACIÓN DE LA NORMA ISO 27001 PARA EL PROCESO DE PROVISIÓN PARA ARCOM S.A

*PERALTA CASTELLANOS, Oscar David*

#### **PALABRAS CLAVE**

Norma, implementación, proceso, NORMA ISO 2107, empresa.

#### **DESCRIPCIÓN**

Las tecnologías de la información son la base sustentable de los procesos estratégicos, la cual se propende por exhaustivos procesos de implementación. Con el paso del tiempo se están creando nuevos sistemas de almacenamiento de información virtuales como lo son servidores dedicados, Cloud Computing<sup>1</sup> entre otros, en estos sistemas está documentado la mayoría de la información de las empresas por medio de interfaces graficas de uso exclusivo de la empresa en la cual se implemente. Con el uso de estas interfaces se garantiza que solo puede acceder a la información el personal que está involucrado en el proceso, como también se garantiza que la información de carácter corporativo está a salvo. Las empresas proveedoras en tecnologías de la información con el afán de garantizar a sus clientes que toda la información que el cliente les suministre y la información que la misma empresa tiene en la solución de problemas, certifican sus procesos con estándares internacionales como garantía de que la información suministrada por el cliente como la información propia de la empresa está a salvo y ajena que delincuencia cibernética la

cual pueda obtener esta información de carácter confidencial.

Es por esto que las empresas ven la importancia de certificarse en el caso colombiano en normas ICONTEC / ISO / IEC, normas de estandarización internacionales que garantizan al cliente la responsabilidad y compromiso en el desarrollo de sus procesos internos.

ARCOM S.A empresa en telecomunicaciones con cinco años de experiencia está en la necesidad de garantizar a sus clientes el buen manejo y uso de las tecnologías de la información es por ello el interés de certificar el departamento de provisión en la norma ISO 27001 la cual implementa un Sistema de Gestión de Seguridad de la Información como modelo piloto para la certificación después de todas las áreas que componen la empresa.

#### **FUENTES**

Se consulta la Norma ISO 27001, los documentos escritos por RODRIGO FERRER (2008) sobre Metodología de análisis de riesgo y sistema de gestión de seguridad de la información SGSI. Se considera el libro de **JOSE MANUEL POVEDA (2010)** Definición de las políticas, organización, alcance del sistema de gestión y concienciación

#### **CONTENIDO**

Se presentan diez capítulos correspondientes en los que se encuentra el Planteamiento del problema, justificación, objetivos, antecedentes, marco

informáticos (redes, servidores, almacenamiento, aplicaciones, etc.) que pueden ser rápidamente dispuestos con un esfuerzo mínimo por parte del proveedor de estos recursos”

---

<sup>1</sup>La Asociación Colombiana de Ingenieros de Sistemas define Cloud Computing como.  
“Modelo que proporciona de manera conveniente, acceso por demanda a un conjunto compartido y configurable de recursos

teórico, introducción a ISO 27001, proceso de planeación propuesto, se describe el procedimiento para la implementación de la Norma ISO27001 en ARCOM S.A. dentro del documento se presenta el organigrama de la organización y sus diferentes departamentos en los cuales será aplicado, roles perfiles y funciones. Se describen las condiciones físicas y técnicas del área de la compañía, alcances limitaciones, metodología, impactos, amenazas, vulnerabilidades y las conclusiones.

## **METODOLOGÍA**

ARCOM S.A empresa con 5 años de experiencia en el sector de las telecomunicaciones en la actualidad maneja diferentes proyectos para su cliente principal Claro Soluciones Fijas, estos proyectos consisten en el monitoreo, soporte técnico, implementación de servicios para los diferentes clientes corporativos con los que cuenta esta compañía.

Es por esto y con el fin de brindar mejor servicio a su principal cliente que en ARCOM S.A surge la necesidad de certificar todos los procesos tanto administrativos como técnicos basados en la norma ISO 9001<sup>2</sup> , ISO IEC 20000<sup>3</sup> en todas las dependencias técnicas y administrativas de las que ARCOM S.A se compone<sup>4</sup>. Pero, realizar un proceso de certificación masivo para las distintas dependencias condiciona mucho el éxito de las mismas pues dichos procesos deben ser secuenciales en su proceso de certificación y es por esto que la alta gerencia ha determinado que la implementación de la norma ISO IEC 27001 debe ser aplicada en el área de provisión pues la información que esta dependencia maneja es de carácter confidencial debido a que se maneja la información de las redes de los clientes de nuestro cliente principal Claro Soluciones Fijas por ende la alta gerencia considera que no se le está dando el manejo debido a esta información a causa ya sea por gestión de usuarios en las plataformas usadas por el cliente como el desconocimiento del adecuado uso de las Tecnologías de la Información.

Teniendo en cuenta lo anteriormente dicho es necesario aclarar que todas las dependencias que componen ARCOM S.A son igual de importantes

a el área de implementación de servicios provisión, la alta dirección determina que aplicar tres normas ISO paralelamente en todas las dependencias de la empresa sería un riesgo muy alto pues se saturaría las funciones del departamento de calidad y con esto conllevaría a la no obtención de ninguno de los tres certificado los cuales la empresa quiere implementar, por ende se determina la obtención de la certificación ISO 27001 de manera secuencial empezando por el área de implementación de servicios y provisión hasta lograr implementar la norma en todas las demás dependencias

## **CONCLUSIONES**

La implementación de la norma técnica ISO 27001 es aplicable en cualquier entorno laboral donde se quieran mejorar las prácticas en el manejo de tecnologías de la información, debido a que en la actualidad la información ya dejó de ser netamente documentada por el contrario ahora la información es manejada virtualmente, almacenada en servidores dedicados y se puede consultar de manera segura como el uso de intranet o servidores por medio de protocolos de transferencia.

La participación del personal involucrado en procesos de certificación es vital, debido a que ellos son los encargados de aplicarlas y de manipular de forma correcta la información, en el proceso de implementación de la norma es necesario el trabajo en conjunto con el personal de calidad que esté llevando el proceso, es por esto que los más interesados en la aplicación de la norma son el personal del área quienes son los directamente beneficiados en dicho proceso.

En el caso de ARCOM S.A una empresa dedicada a la tercerización de servicios se hace un poco más complejo la aplicación de la norma debido a que en el caso de los programas de gestión y configuración de redes se hace más difícil que los clientes respondan los requisitos de manera ágil y eficiente lo cual entorpece un poco la implementación de la norma.

El reconocimiento de amenazas y vulnerabilidades en el área de implementación de servicios y provisión se torna en algunos momentos subjetiva debido que algunos tópicos en los cuales para el

---

<sup>2</sup>NORMA ISO 9001 SISTEMA DE GESTION DE CALIDAD

<sup>3</sup>NORMA ISO 20000 TECNOLOGÍAS DE LA INFORMACIÓN

<sup>4</sup> Dependencias Administrativas y Técnicas tipificadas en el organigrama figura No.2



área de seguridad es crítico y merece de especial apoyo por parte de provisión, el personal de implementación de servicios no le ven la criticidad ya indicada, es por eso que algunas amenazas y vulnerabilidades no quedaron registrados en el proyecto.

El proceso de certificación de la norma ISO 27001, tiene una especial afinidad con la ingeniería de telecomunicaciones pues se implementan y se generan procesos los cuales en el área son recientes y que abarcan una gran cantidad de información y conocimientos que en el oficio de la ingeniería de telecomunicaciones es un complemento vital en el proceso de ser profesional integral.

La aplicación de esta norma técnica en empresas que quieran controlar y mejorar el uso de las tecnologías de información, humaniza un poco el

uso de las tecnologías debido a que por medio de estas estructuras estamos conociendo y tomando controles los cuales promueven la seguridad de la información.

El proceso de certificación es un proceso en el cual muchas dependencias de la empresa se unen por un bien común, lo cual en el ámbito laboral y humano estrecha y fortalece las relaciones interpersonales de los funcionarios lo cual mejora notablemente el ámbito laboral, social y personal.

La consecución de la norma ISO 27001 es un logro de todo el personal involucrado en dicho proceso, lo que refleja la importancia del trabajo en grupo donde todos hacen pieza importante en el proceso de certificación lo cual fortalece e impulsa a trabajar por un proyecto que es reconocido a nivel internacional

**IMPLEMENTACIÓN EN LA FASE  
DE PLANEACIÓN DE LA NORMA ISO 27001 PARA EL PROCESO DE  
PROVISIÓN PARA ARCOM S.A**

**OSCAR DAVID PERALTA CASTELLANOS**

**CORPORACIÓN UNIVERSITARIA UNITEC  
ESPECIALIZACIÓN GERENCIA DE PROYECTOS  
SEMINARIO DE INVESTIGACIÓN II  
BOGOTÁ D.C., FEBRERO DE 2018  
CORPORACIÓN UNIVERSITARIA UNITEC  
CENTRO DE INVESTIGACIÓN**

El consejo de la Facultad de Ingeniería, en sesión para temas de investigación, hace constar que; previa análisis y discusión de resultado de evaluación de jurados, otorgó al trabajo titulado: **IMPLEMENTACIÓN EN LA FASE DE PLANEACIÓN DE LA NORMA ISO 27001 PARA EL PROCESO DE PROVISIÓN PARA ARCOM S.A”**

**La calificación de APROBADO**

Para optar el título de Especialista en Gerencia de Proyectos.

Para constancia se firma a los 12 días del mes de febrero de 2018.

---

*Jorge Humberto Torres Zea*

*Coordinador Educación a Distancia y Virtual*

**TABLA DE CONTENIDO**

<b>INTRODUCCIÓN</b>	6
<b>PLANTEAMIENTO DEL PROBLEMA</b>	8
<b>JUSTIFICACIÓN</b>	9
<b>OBJETIVO PRINCIPAL</b>	10
<b>OBJETIVOS ESPECÍFICOS</b>	10
<b>ANTECEDENTES</b>	11
<b>MARCO TEÓRICO</b>	13
<b>INTRODUCCIÓN A ISO 27001</b>	13
<b>PROCESO DE PLANEACIÓN NORMA ISO 27001</b>	14
<b>DEFINICIÓN ALCANCE SGCI</b>	15
<b>METODOLOGÍA DE EVALUACIÓN DE RIESGO</b>	15
<b>INVENTARIO DE ACTIVOS</b>	16
<b>IDENTIFICAR AMENAZAS Y VULNERABILIDADES</b>	16
<b>IDENTIFICAR IMPACTOS</b>	17
<b>ANÁLISIS Y EVALUACIÓN DEL RIESGO</b>	17
<b>SELECCIÓN DE CONTROLES</b>	18

**PROCEDIMIENTO PARA LA IMPLEMENTACIÓN DE LA NORMA ISO 27001**

<b>ARCOM S.A.</b>	- 18 -
<b>ÁREA DE IMPLEMENTACIÓN DE SERVICIOS DE ARCOM S.A</b>	19
<b>CONOCIMIENTOS Y HABILIDADES:</b>	20
<b>COORDINADOR DE IMPLEMENTACIÓN DE SERVICIOS</b>	20
<b>INGENIERO DE APOYO PEM</b>	20
<b>SERVICIOS EN TELECOMUNICACIONES</b>	20
<b>FUNCIONES Y PERFILES PROFESIONALES</b>	22
<b>COORDINADOR DE IMPLEMENTACIÓN</b>	22
<b>INGENIERO PUESTA EN MARCHA</b>	22
<b>INGENIERO DE CONFIGURACIÓN</b>	23
<b>INGENIERO DE APOYO PUESTA EN MARCHA</b>	24
<b>CONDICIONES FÍSICAS Y TÉCNICAS DEL ÁREA DE IMPLEMENTACIÓN DE SERVICIOS Y PROVISIÓN DE ARCOM S.A</b>	24
<b>CONDICIONES FÍSICAS</b>	24
<b>CONDICIONES TÉCNICAS</b>	25
<b>PROGRAMAS Y APLICATIVOS</b>	25
<b>NORMA ISO 27001 APLICADO AL ÁREA DE IMPLEMENTACIÓN DE SERVICIOS Y PROVISIÓN ARCOM S.A</b>	27
<b>DEFINICIÓN ALCANCE SGSI</b>	27

<b>DEFINICIÓN DE POLÍTICAS DE SEGURIDAD</b>	29
<b>ALCANCES Y LIMITACIONES</b>	31
<b>ALCANCES</b>	31
<b>LIMITACIONES</b>	32
<b>ENFOQUE HUMANÍSTICO</b>	33
<b>DELIMITACIÓN</b>	35
<b>DELIMITACIÓN CRONOLÓGICA</b>	35
<b>DELIMITACIÓN ESPACIAL</b>	35
<b>DELIMITACIÓN ECONÓMICA</b>	35
<b>METODOLOGÍA DE EVALUACIÓN DE RIESGOS</b>	36
<b>INVENTARIO DE ACTIVOS</b>	40
<b>IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES</b>	42
<b>IDENTIFICAR IMPACTOS</b>	43
<b>ANÁLISIS Y EVALUACIÓN DE RIESGOS</b>	44
<b>SELECCIÓN DE CONTROLES</b>	46
<b>CONCLUSIONES</b>	49
<b>BIBLIOGRAFÍA</b>	51

## INTRODUCCIÓN

Las tecnologías de la información son la base sustentable de los procesos estratégicos, la cual se propende por exhaustivos procesos de implementación. Con el paso del tiempo se están creando nuevos sistemas de almacenamiento de información virtuales como lo son servidores dedicados, Cloud Computing<sup>5</sup> entre otros, en estos sistemas está documentado la mayoría de la información de las empresas por medio de interfaces graficas de uso exclusivo de la empresa en la cual se implemente. Con el uso de estas interfaces se garantiza que solo puede acceder a la información el personal que está involucrado en el proceso, como también se garantiza que la información de carácter corporativo está a salvo.

Pero con el tiempo y a medida que la información con mayor importancia está confinada en estos sistemas de almacenamiento virtuales la delincuencia informática ha ido avanzando con el fin obtener información ajena para el uso indebido de la misma, es por esto que existen parámetros de seguridad que se implementan para salvaguardar esta información que han sido aplicados por las empresas.

Las empresas proveedoras en tecnologías de la información con el afán de garantizar a sus clientes que toda la información que el cliente les suministre y la información que la misma empresa tiene en la solución de problemas, certifican sus procesos con estándares internacionales como garantía de que la información suministrada por el cliente como la información propia de la empresa está a salvo y ajena que delincuencia cibernética la cual pueda obtener esta información de carácter confidencial.

Es por esto que las empresas ven la importancia de certificarse en el caso colombiano en normas ICONTEC / ISO / IEC, normas de estandarización internacionales que garantizan al cliente la responsabilidad y compromiso en el desarrollo de sus procesos internos.

---

<sup>5</sup>La Asociación Colombiana de Ingenieros de Sistemas define Cloud Computing como. “Modelo que proporciona de manera conveniente, acceso por demanda a un conjunto compartido y configurable de recursos informáticos (redes, servidores, almacenamiento, aplicaciones, etc.) que pueden ser rápidamente dispuestos con un esfuerzo mínimo por parte del proveedor de estos recursos”

ARCOM S.A empresa en telecomunicaciones con cinco años de experiencia está en la necesidad de garantizar a sus clientes el buen manejo y uso de las tecnologías de la información es por ello el interés de certificar el departamento de provisión en la norma ISO 27001 la cual implementa un Sistema de Gestión de Seguridad de la Información como modelo piloto para la certificación después de todas las áreas que componen la empresa.

## **PLANTEAMIENTO DEL PROBLEMA**

La información se considera como un activo intangible, pero a su vez es el activo más importante con el que cuenta una compañía, es por esto que el daño, pérdida, manipulación indebida de este activo trae consecuencias nefastas para para las empresas.

Cuando las Tecnologías de la información y las comunicaciones permearon en la empresas y grandes industrias, se encontró en ellas un método en el cual la información pasaba de ser algo tangible y cuantitativo en algo que estaba alojado de manera virtual en plataformas seguras en donde tiene una protección adecuada.

Aterrizando el proyecto a lo realizado durante la práctica como ingeniero de apoyo puesta en marcha en ARCOM S.A la manipulación de la información en el área de provisión de la empresa, era netamente informática que por medio de una base de datos exclusiva de Claro Soluciones Fijas y de empresas prestadoras de servicios como en el caso de ARCOM S.A estaba establecida toda la información para los diferentes proyectos que Claro ejecutaba en todo el país, base de datos la cual siempre se está alimentando con información nueva de clientes que quieren adquirir servicios en telecomunicaciones.

Es por esto que el proceso de provisión de ARCOM S.A se ve en la necesidad de certificar con estándares internacionales que los procesos se están ejecutando de manera correcta dando una manipulación a la información adecuada de tal manera que esta no sea manipulada o hurtada. También se garantiza por medio de la verificación de estos procesos el personal de provisión está capacitado y es consciente que el manejo la información y de su importancia tanto para Claro Soluciones Fijas que en este caso es el proveedor del servicio como la información del cliente quien está interesado en adquirir el servicio.

Es prioridad para el proceso de provisión ARCOM S.A dar a conocer que sus clientes pueden confiar su información y que se cuenta con tecnología, condiciones físicas, condiciones ambientales y personal capacitado en dar gestión y soporte a las redes de los cliente teniendo métricas establecidas, políticas y controles adecuados para que la información del cliente y de ARCOM S.A tenga un porcentaje de aceptación del riesgo aceptable para las partes.

## JUSTIFICACIÓN

Las tecnologías de la información han permeado en las empresas de cualquier razón social de manera exitosa y en poco tiempo, pues de esta manera la información logra una inmediatez que optimiza el trabajo y los resultados a corto plazo, ya con el tiempo se evidencia que distintos métodos de almacenamientos físicos de la información, tales como la gestión documental se convertiría en una amenaza para la información, pues la manipulación inadecuada y las condiciones ambientales no permiten la preservación de la información.

La seguridad de la información basada en el contexto de las tecnologías de información está estandarizada por normas y estándares internacionales las cuales parametriza la unión entre la información, los usuarios a cargo de la información y los funcionarios que intervienen en el proceso de la información, es por esto que es necesario implementar estándares donde la información garantice en un alto porcentaje que está segura, es evidente que no hay una garantía total donde la información no sea vulnerable pero debe haber un porcentaje el cual sea aceptable asumirlo.

La implementación de la norma ISO 27001 para ARCOM S.A una empresa aliada para Claro Soluciones Fijas Colombia, es importante pues se le da soporte y provisión a la empresa dominante en el área de telecomunicaciones en soluciones fijas en todo Colombia, por lo que esta compañía requiere la información corporativa confidencial como la de sus clientes sean manipulados y modificados por personal capacitado garantizando que la información y procesos que se están tercerizando estén seguros y con esto Claro Soluciones Fijas este enfocado en su objetivo principal.

### **OBJETIVO PRINCIPAL**

Implementar y documentar la norma ISO 27001 aplicada en el departamento de implementación de servicios y provisión de la empresa ARCOM S.A.

### **OBJETIVOS ESPECÍFICOS**

- Durante el periodo de desarrollo de la pasantía poder realizar un trabajo completo en el cual sea útil y aplicable a la empresa como también sea un método de enseñanza para el estudiante.
- Aplicar los conocimientos adquiridos durante el periplo de estudiante en 10 semestres en Ingeniería de Telecomunicaciones en la Universidad o, en el ámbito técnico y administrativo de las telecomunicaciones.
- Concientizar al personal del área de provisión de ARCOM S.A acerca del buen uso de las Tecnologías de la Información y de la importancia de la seguridad de la información.

## ANTECEDENTES

La norma ISO IEC 27001 tiene la característica de ser una norma que abarca todo tipo de organizaciones en la página oficial de la norma la define como “Esta norma especifica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener, y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización”

Esta norma se diseñó con el fin de garantizar la selección óptima de controles de seguridad los cuales mitiguen en un porcentaje aceptable por la alta dirección los activos de información logrando con esto que la información este a salvo.

La norma ISO IEC 27001 establece normas genéricas las cuales tienen como propósito ser aplicables en cualquier tipo de empresa con cualquier razón social, sin depender de la estructura de negocio, capacidad de personal, razón social o jurídica de la empresa entre otras características.

Es importante acotar que para la aplicación de la norma se hace necesario especificar que dependencias tanto administrativas como técnicas se les va a implementar la norma ISO 27001 y que además justifique y evidencie con documentaciones propias que las dependencias que va a ser excluidas de este proceso de certificación no afecte directamente a los activos de la empresa y que cualquier riesgo o amenaza que éstas puedan generar sean aceptados y avalados por la alta dirección.

La norma ISO 27001 en el siglo XXI está siendo implementada por empresas de telecomunicaciones pues la información está siendo con el tiempo más confiada a las redes de telecomunicación y discos duros virtuales los cuales economizan espacio físico, recurso humano y riesgo de que la información sea vulnerable a alguna amenaza o riesgo.

La norma ISO 27001 debe ser implementada en cuatro procesos los cuales son:

- Planear
- Actuar
- Hacer
- Verificar

La planeación es el proceso más importante en este ciclo pues es donde se recoge la información de la empresa, los actores de los procesos y donde se analizan los riesgos y así mismo los controles los cuales deben ser escogidos acorde a la norma y avalados por la alta dirección de la empresa.

## MARCO TEÓRICO

### INTRODUCCIÓN A ISO 27001

La norma ISO IEC 27001 tiene la característica de ser una norma que abarca todo tipo de organizaciones en la página oficial de la norma la define como “Esta norma especifica los requisitos para establecer, implementar, operar, hacer seguimiento, revisar, mantener, y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización”

Esta norma se diseñó con el fin de garantizar la selección optima de controles de seguridad los cuales mitiguen en un porcentaje aceptable por la alta dirección los activos de información logrando con esto que la información este a salvo.

La norma ISO IEC 27001 establece normas genéricas las cuales tienen como propósito ser aplicables en cualquier tipo de empresa con cualquier razón social, sin depender de la estructura de negocio, capacidad de personal, razón social o jurídica de la empresa entre otras características.

Es importante acotar que para la aplicación de la norma se hace necesario especificar que dependencias tanto administrativas como técnicas se les va a implementar la norma ISO 27001 y que además justifique y evidencia con documentaciones propias que las dependencias que va a ser excluidas de este proceso de certificación no afecte directamente a los activos de la empresa y que cualquier riesgo o amenaza que éstas puedan generar sean aceptados y avalados por la alta dirección.

La norma ISO 27001 en el siglo XXI está siendo implementada por empresas de telecomunicaciones pues la información está siendo con el tiempo más confiada a las redes de telecomunicación y discos duros virtuales los cuales economizan espacio físico, recurso humano y riesgo de que la información sea vulnerable a alguna amenaza o riesgo.

La norma ISO 27001 debe ser implementada en cuatro procesos los cuales son:

- Planear
- Actuar
- Hacer
- Verificar

La planeación es el proceso más importante en este ciclo pues es donde se recoge la información de la empresa, los actores de los procesos y donde se analizan los riesgos y así mismo los controles los cuales deben ser escogidos acorde a la norma y avalados por la alta dirección de la empresa.

### PROCESO DE PLANEACIÓN NORMA ISO 27001

Figura No.1 Esquema de proceso de planeación norma ISO 27001<sup>6</sup>



FUENTE: AUTOR

<sup>6</sup>INSTITUTO COLOMBIA DE NORMAS TÉCNICAS

## **DEFINICIÓN ALCANCE SGCI**

- Definir que se quiere proteger y el alcance que se le va a dar al sistema.
- Definir límites del SGSI, características de la organización (objeto social), localización, tecnologías implementadas, activos.
- Definir en qué departamentos se va a implementar el SGSI, y cuales departamentos quedan excluidos y justificarlo.

## **DEFINIR POLÍTICAS DE SEGURIDAD**

- La política de seguridad se define como un manifiesto por parte de la dirección en la cual expresa apoyo y compromiso con la seguridad de la información, alineados en los objetivos de la empresa como también en la legislación vigente.
- Dicho manifiesto debe ser dirigido y publicado a todo el personal interno como externo involucrado en el proceso con el fin de que el comunicado no pierda su importancia y plasme el apoyo por parte de la dirección en el arranque del proceso.

## **METODOLOGÍA DE EVALUACIÓN DE RIESGO**

- Se establece como el activo más importante que es la información está siendo utilizado mirando diferentes aspectos como:
  - Medios de transmisión
  - Funcionarios que intervienen en el proceso
  - Origen y destino de la información
- Bajos estas premisas se comienza un proceso de análisis identificando posibles riesgos y vulnerabilidades en el trayecto de la información.

## **INVENTARIO DE ACTIVOS**

- Proceso en el cual se deben identificar todos los activos, registrarlos en una base de datos e irlos actualizando de manera periódica como también registrando en back up.
- En este parte del proceso se debe documentar la importancia de cada uno de los activos, con datos tales como:
  - Tipo de Activo
  - Formato
  - Ubicación
  - Información sobre soporte técnico
  - Información de licencias
- Se debe documentar quien es el “propietario” del equipo, con propietario refiérase al funcionario que se le fue asignado ese activo, dar un valor de que te tan importante y valiosa es esa información para la empresa, y determinar los niveles de protección para la misma.

## **IDENTIFICAR AMENAZAS Y VULNERABILIDADES**

- Las amenazas se pueden calificar de la siguiente manera:
  - Amenazas Humanas
  - Amenazas Ambientales
- Valiéndose de la anterior calificación se debe desglosar e identificar de que manera la información está corriendo un riesgo, la norma las clasifica como:
  - Amenazas humanas
  - Amenazas Accidentales
- Las vulnerabilidades se define como la debilidad de un activo, que puede ser vulnerada y aprovechada por una amenaza, las vulnerabilidades actúan en conjunto

de por si la existencia de una sola vulnerabilidad no logra en si ser un riesgo para la información. Un ejemplo práctico es la no creación de usuarios en el uso de alguna plataforma virtual, el hecho de que no se gestionen a tiempo los usuarios y contraseñas permiten que ante una amenaza humana que quiera afectar la información se establezca un riesgo.

## **IDENTIFICAR IMPACTOS**

- Ya identificados las amenazas y vulnerabilidades se deben analizar que impactos traen estas y que grado de afectación pueda poner en riesgo a la información, al identificar los impactos se está determinando en que grado esas amenazas y vulnerabilidades pueden también afectar los objetivos del negocio.

## **ANÁLISIS Y EVALUACIÓN DEL RIESGO**

- Basados en los objetivos del negocio los riesgos se deben calificar y cuantificar esto con el fin de determinar que riesgos son prioritarios y que controles se deben aplicar. Los riesgos se pueden tratar de tres formas:
  - Asumen
  - Mitigan
  - Transfieren
- Los riesgos pueden ser transferidos en el caso de que este no este alineado con los objetivos del negocio.
- Se asumen cuando el riesgo afecta de manera directa con la información y esta afecta los alineamientos del negocio.
- Se mitigan si el riesgo residual es considerablemente bajo, pero la información puede estar aun en riesgo

**Una política o control nunca eliminara un riesgo, siempre existirá un riesgo residual que debe ser aceptado por parte de la dirección**

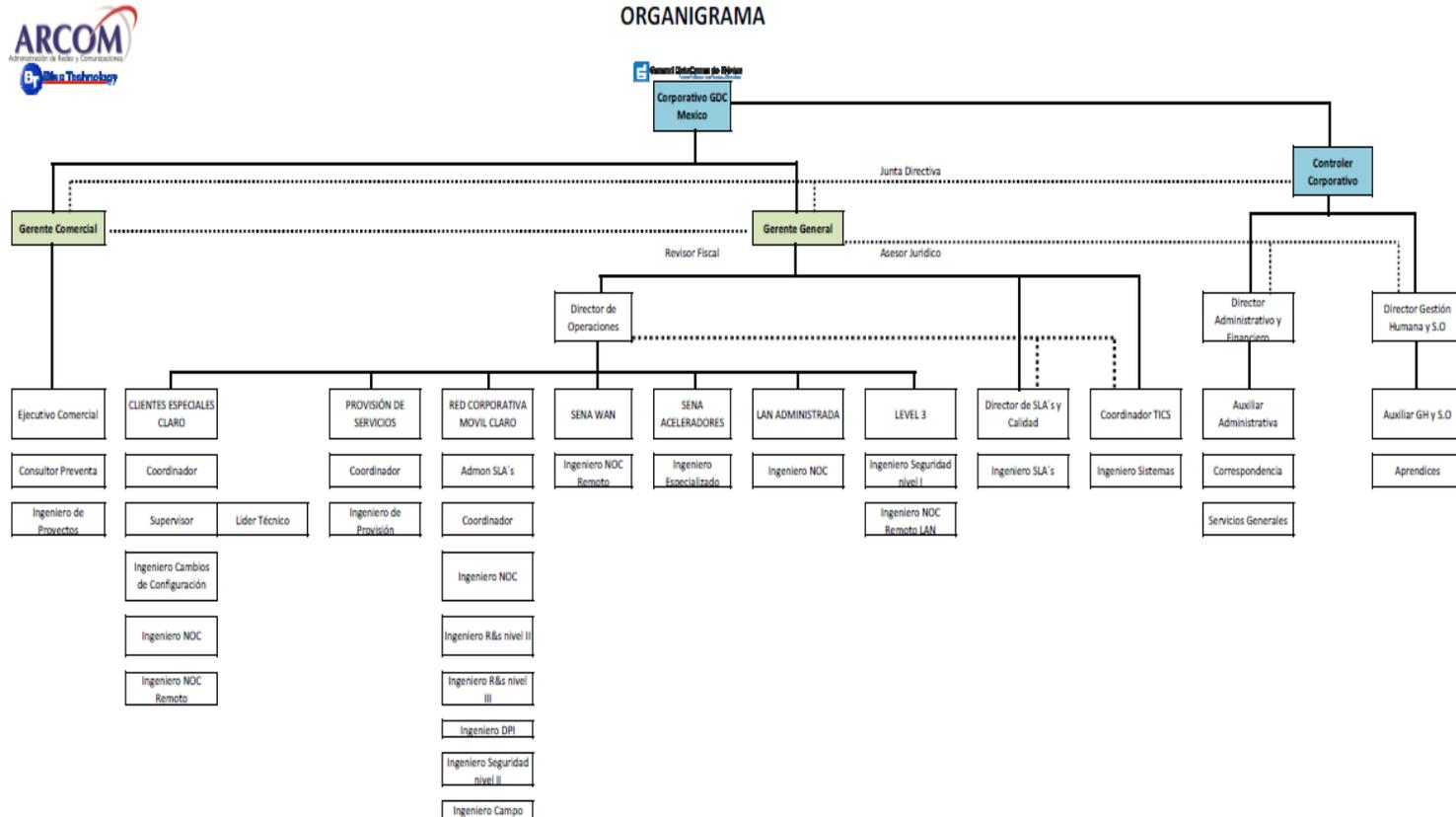
## SELECCIÓN DE CONTROLES

- Cuando se tienen identificados todos los riesgos se deben seleccionar los controles necesarios para que el riesgo residual este en un nivel aceptable que la gerencia acepte y esté dispuesta a asumir. Los controles están establecidos de estas dos maneras:
  - La norma ISO 27001 en el anexo a registra un cuadro de controles los cuales pueden ser usados y si estos reducen el nivel de riesgo considerablemente.
  - Se pueden crear controles que se ajusten a los riesgos, siempre y cuando estén alineados con la regulación nacional como internacional

## MARCO METODOLÓGICO

### PROCEDIMIENTO PARA LA IMPLEMENTACIÓN DE LA NORMA ISO 27001 ARCOM S.A.

#### Organigrama de ARCOM S.A y departamentos administrativos y técnicos de la empresa

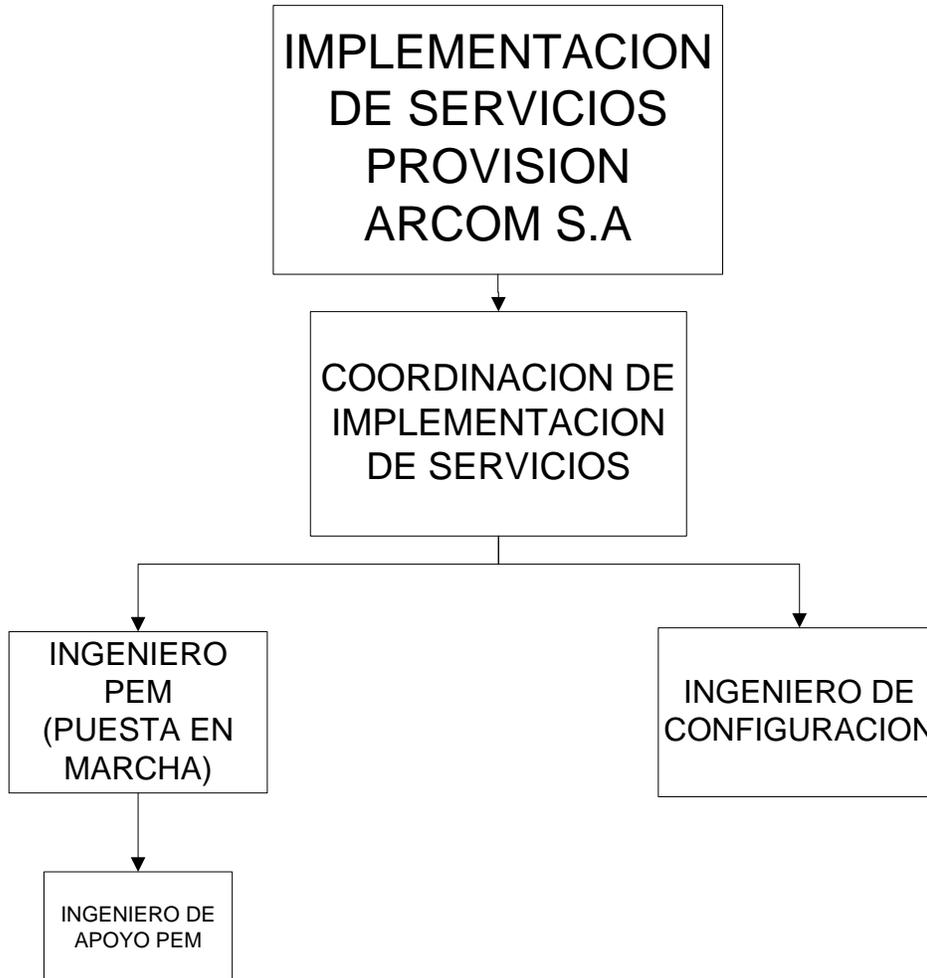


Fuente: ARCOM S.A

## ÁREA DE IMPLEMENTACIÓN DE SERVICIOS DE ARCOM S.A

El área de provisión de ARCOM S.A está constituida de la siguiente manera:

Figura No.2 Área de Implementación de Servicios y Provisión ARCOM S.A



FUENTE: AUTOR

El área de implementación de servicios de ARCOM S.A es el encargado de realizar configuración y entregar servicios para clientes corporativos de la empresa Claro Soluciones Fijas.

El área de provisión de servicios de ARCOM S.A en la actualidad se compone de:

- 1 Coordinador de implementación de servicios
- 6 Ingenieros PEM (Puesta en Marcha)
- 1 Ingeniero de configuración
- 1 Ingeniero de apoyo PEM

## **CONOCIMIENTOS Y HABILIDADES:**

### **COORDINADOR DE IMPLEMENTACIÓN DE SERVICIOS**

Conocimientos Técnicos en:

- Servicios de Datos
- Telefonía
- Transmisión
- Servicios en PBX Administradas

Conocimientos Administrativos en:

- Manejo de personal
- Manejos de Proyectos
- Conocimientos en ITIL (Information Technology Infrastructure Library)

### **INGENIERO PUESTA EN MARCHA E INGENIERO DE CONFIGURACIÓN**

- Servicios de datos
- Servicios de voz
- Servicios de PBX administradas
- Videoconferencia
- SDH

### **INGENIERO DE APOYO PEM**

- Conocimientos básicos en telecomunicaciones
- Manejo de Office

### **SERVICIOS EN TELECOMUNICACIONES**

El área de provisión da soporte en los siguientes servicios en telecomunicaciones:

- Servicios de Datos

- Servicios de voz
- Servicios de PBX Administrada
- Videoconferencia
- SDH

Los servicios anteriormente mencionados son servicios en telecomunicaciones los cuales Claro Soluciones fijas ofrece en su portafolio corporativo, dichos servicios se dividen en otros servicios más específicos los cuales en la figura 3, a continuación, se explica.

Figura No.3 Servicios ofrecidos por el área de provisión de ARCOM S.A



FUENTE: ÁREA DE PROVISIÓN DE SERVICIOS CLARO SOLUCIONES FIJAS

Para estos servicios ARCOM S.A dispone de personal capacitado y con experiencia en la implementación y configuración de todos estos servicios, lo cual ha brindado garantía y calidad con el transcurso de los años a Claro Soluciones Fijas y ha afianzado con el tiempo nuevas alianzas y tercerización de más procesos de vital importancia para sus clientes.

## **FUNCIONES Y PERFILES PROFESIONALES**

### **COORDINADOR DE IMPLEMENTACIÓN**

Funciones:

- Coordinación y distribución de carga laboral den la carga laboral del grupo para el cumplimiento de las metas diarias asignadas por Claro Soluciones Fijas, en la configuración y puesta en marcha de nuevos servicios.
- Elaboración de reportes diarios y mensuales sobre la evolución, desempeño, efectividad y cumplimiento de las actividades realizadas por el área, conciliación y facturación de las mismas.
- Desarrollo de procesos en pro de la organización y mejora continua del área, metas y objetivos planteados con Claro Soluciones Fijas a cumplir durante la realización del proyecto a cargo.
- Soportar procesos de escalamiento con personal de Claro Soluciones Fijas.

### **INGENIERO PUESTA EN MARCHA**

El ingeniero puesta en marcha debe llevar a cabo actividades las cuales previo desarrollo y planificación es la parte final en la entrega de un nuevo servicio a un cliente, por ende es un cargo de alta responsabilidad el cual debe ser ejecutado con compromisos por parte del ingeniero logrando con esto que el cliente final de Claro Soluciones Fijas obtenga un servicio garantizado, como el cliente directo de ARCOM S.A, Claro Soluciones Fijas en una nueva soluciona a nuevos servicios que se deben entregar.

Funciones:

- Previa información y revisión de documentación acerca de la actividad que se va a entregar, revisando tópicos como configuraciones realizadas, confirmación de condiciones eléctricas habilitadas, ingeniera de detalle y documentos anexos.

- Realizar pruebas de servicios y conexiones previas verificando conectividad con los equipos del cliente.
- Documentar las pruebas realizadas teniendo en cuenta fecha, hora, personal que se desplazó por parte de Claro Soluciones Fijas para la instalación de equipos en la sede del cliente y anotaciones relevantes que puedan afectar la prestación del servicio al cliente final.
- En caso tal de que hayan inconvenientes de conectividad, equipos, disponibilidad del cliente, deben ser informados y documentados dichos sucesos a personal de claro que está al tanto de la instalación, estos escalamientos están parametrizados por unos tiempos de ejecución para lograr resolver los problemas según su estado de gravedad, y entregar el servicio satisfactoriamente.

## **INGENIERO DE CONFIGURACIÓN**

El ingeniero de configuración es el encargado de configurar los servicios que el cliente solicita para esto debe tener en cuenta los siguientes parámetros:

- Debe documentarse acerca de qué servicio solicita el cliente, donde se encuentra ubicado y en que servidores y ciudades se va a configurar el servicio.
- Configuraciones técnicas tales como creación y verificación de VRF (Librerías de red virtuales), configuración de MPLS, configuración de switch, dependiendo del servicio que el cliente requiera.
- Configuración de servicios en PBX Administradas.
- Documentación de las actividades ejecutadas y los puertos, redes, VRF configuradas para el servicio requerido.

## **INGENIERO DE APOYO PUESTA EN MARCHA**

El ingeniero de apoyo puesta en marcha es el encargado de documentar y de estar pendiente de inconvenientes técnicos y administrativos básicos que impidan iniciar el desarrollo correcto de la actividad.

- Debe establecer comunicación antes de la hora programada con los ingenieros de campo que están en los diferentes clientes con el fin de establecer hora de llegada y confirmarles acompañamiento por parte del área de provisión de ARCOM S.A.
- Es el encargado de confirmar condiciones eléctricas adecuadas para poder instalar equipos y que estos funcionen de manera correcta.
- En caso dado de que surjan inconvenientes tanto de ingreso como técnico, se deben realizar escalamientos en tu tiempo determinado con el fin de que se puedan solucionar en el menor tiempo posible y la actividad pueda ser entregada satisfactoriamente.
- Documentar las actividades realizadas durante el día y facturarlas esto con el fin que el coordinador del área de provisión tenga control de la facturación diaria del departamento.

## **CONDICIONES FÍSICAS Y TÉCNICAS DEL ÁREA DE IMPLEMENTACIÓN DE SERVICIOS Y PROVISIÓN DE ARCOM S.A**

### **CONDICIONES FÍSICAS**

Con el fin de poder brindar el mejor servicio en la implementación de servicios el área de implementación de servicios y provisión cuenta con una completa área de sistemas el cual en la calle 13 A No. 89-38 en la oficina 604.

## CONDICIONES TÉCNICAS

El área técnica de implementación de servicios y provisión cuenta con:

- Computadores HP S1933
- Teléfonos Cisco IP Phone 7960
- Teléfonos celulares Nokia 2710
- Servidor Windows XP

En el uso de software se dispone de los programas que utilizan Claro Soluciones Fijas quienes otorgan las licencias de uso de estos programas para los distintos servicios que se configuren.

El uso de este software es lo que impulsa a ARCOM S.A y al área de implementación de servicios de provisión a certificarse en la norma ISO 27001 pues el uso de dicho software por parte de Claro Soluciones Fijas ha llevado al no correcto uso de las Tecnologías de la Información y que el acceso inseguro a las redes de los clientes.

## PROGRAMAS Y APLICATIVOS

- Servicio de acceso a capa 3<sup>7</sup> Red:
  - Nombre del software: 5620 SAM Client App  
Versión: Release 9.0  
Fabricante: Alcatel Lucent
  - Nombre del software: Control de Acceso Unificado  
Versión: 1.0.0.8  
Fabricante: ONYX Customer
  
- Servicio de datos:

---

<sup>7</sup>Según el Modelo ISO la capa 3 de red encarga de direccionar y gestionar el tráfico de paquetes que se envían.

- Nombre del software: PuTTY Connection Manager  
Versión: 7.0.1 Beta  
Fabricante: PuTTY Connection Manager
  
- Nombre del software: E managment  
Versión:  
Fabricante: Claro Soluciones Fijas
  
- Servicios de voz:
  - Nombre del software: Local Maitenance Terminal  
Versión: 1.0  
Fabricante: Huawei
  
- Servicios de PBX administradas:
  - Nombre del software: CISCO Unified CM Administration  
Versión: 7.1.5.34.058-1  
Fabricante: CISCO
  
- Servicios de videoconferencia:
  - Nombre del software: TANDBERG  
Versión:  
Fabricante: TANDBERG
  
- Servicios SDH:
  - Nombre del software: U2000  
Versión: 1.0.0.8  
Fabricante: HUAWEI

## **NORMA ISO 27001 APLICADO AL ÁREA DE IMPLEMENTACIÓN DE SERVICIOS Y PROVISIÓN ARCOM S.A**

Según lo explicado en la figura No.1 en el Esquema de proceso de planeación norma ISO 27001 la norma indica seguir dichos procesos documentados bajos unos numerales los cuales están estipulados en la norma.

### **DEFINICIÓN ALCANCE SGSI<sup>8</sup>**

ARCOM S.A empresa con 5 años de experiencia en el sector de las telecomunicaciones en la actualidad maneja diferentes proyectos para su cliente principal Claro Soluciones Fijas, estos proyectos consisten en el monitoreo, soporte técnico, implementación de servicios para los diferentes clientes corporativos con los que cuenta esta compañía.

Es por esto y con el fin de brindar mejor servicio a su principal cliente que en ARCOM S.A surge la necesidad de certificar todos los procesos tanto administrativos como técnicos basados en la norma ISO 9001<sup>9</sup> , ISO IEC 20000<sup>10</sup> en todas las dependencias técnicas y administrativas de las que ARCOM S.A se compone<sup>11</sup>. Pero, realizar un proceso de certificación masivo para las distintas dependencias condiciona mucho el éxito de las mismas pues dichos procesos deben ser secuenciales en su proceso de certificación y es por esto que la alta gerencia ha determinado que la implementación de la norma ISO IEC 27001 debe ser aplicada en el área de provisión pues la información que esta dependencia maneja es de carácter confidencial debido a que se maneja la información de las redes de los clientes de nuestro cliente principal Claro Soluciones Fijas por ende la alta gerencia considera que no se le está dando el manejo debido a esta información a causa ya sea por gestión de usuarios en las plataformas usadas por el cliente como el desconocimiento del adecuado uso de las Tecnologías de la Información.

---

<sup>8</sup> Numeral 4.2.1 de la norma ISO 27001

<sup>9</sup>NORMA ISO 9001 SISTEMA DE GESTION DE CALIDAD

<sup>10</sup>NORMA ISO 20000 TECNOLOGÍAS DE LA INFORMACIÓN

<sup>11</sup> Dependencias Administrativas y Técnicas tipificadas en el organigrama figura No.2

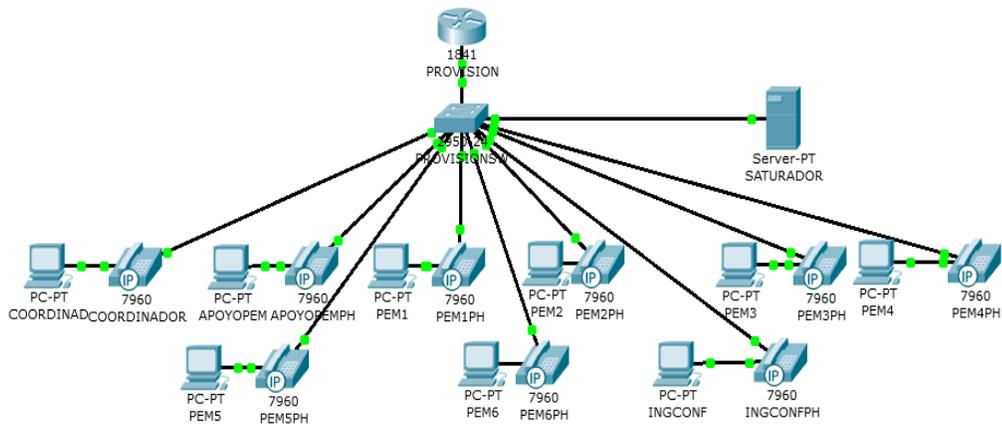
Teniendo en cuenta lo anteriormente dicho es necesario aclarar que todas las dependencias que componen ARCOM S.A son igual de importantes a el área de implementación de servicios provisión, la alta dirección determina que aplicar tres normas ISO paralelamente en todas las dependencias de la empresa sería un riesgo muy alto pues se saturaría las funciones del departamento de calidad y con esto conllevaría a la no obtención de ninguno de los tres certificado los cuales la empresa quiere implementar, por ende se determina la obtención de la certificación ISO 27001 de manera secuencial empezando por el área de implementación de servicios y provisión hasta lograr implementar la norma en todas las demás dependencias.

En el numeral 7.5. “CONDICIONES FÍSICAS Y TÉCNICAS DEL ÁREA DE IMPLEMENTACIÓN DE SERVICIOS Y PROVISIÓN DE ARCOM S.A” están consignadas las condiciones físicas, técnicas, espaciales del área de implementación de servicios y provisión.

La topología de red que se utiliza en el área de provisión es la siguiente:

**TOPOLOGÍA DE RED ÁREA DE IMPLEMENTACIÓN DE SERVICIOS Y PROVISIÓN ARCOM S.A**

Figura No. 4 Topología de red área de implementación de servicios y provisión ARCOM S.A



FUENTE: AUTOR

Esta topología de red es la utilizada en ARCOM S.A la cual cuenta con un router 1841 que le provee servicio de internet y telefonía a toda el área, Claro Soluciones Fijas es el proveedor del servicio, el coordinador del área es la única persona que tiene acceso a la topología de red de manera detallada donde se establece que direcciones IP están asignadas y el funcionamiento de la red como tal, esta información para el proceso de certificación va a tener acceso a todos los integrantes del área de implementación de servicios y provisión con el fin de que tener conocimiento de cómo está funcionando la red e identificar con que amenazas y vulnerabilidades cuenta.

## **DEFINICIÓN DE POLÍTICAS DE SEGURIDAD**

General Datacomm de México proveedor de soluciones de telecomunicaciones en redes y grandes corporativos en Latinoamérica certificado en normas de calidad ISO 9001, ISO IEC 20000, ISO IEC 27001 – 2005, con sedes en México en ciudades como México DF, Guadalajara, Monterrey, Tijuana, Jalapa. En Colombia ARCOM S.A en la ciudad de Bogotá, y en Brasil en la ciudad de Sao Paulo, con el fin de ser una empresa líder en el mercado de las telecomunicaciones en tercerización de soporte de redes y demás soluciones en telecomunicaciones, la alta dirección está interesada en iniciar procesos de certificación en estándares internacionales en las empresas sucursales en Colombia y Brasil con el fin de consolidarse en estos países y empezar un proceso expansionista y poder consolidarse en América Latina.

Es por esto que en Colombia ARCOM S.A está iniciando un proceso el cual de manera global se está llevando a cabo el proceso de certificación en ISO 9001 como también la norma ISO IEC 20000, en donde la familia ARCOM ha mostrado total interés en estos procesos, la participación y aplicación de nuevas maneras de trabajo y nuevas formas de organización ha sido vital en este proceso que está empezando a implementarse.

General Datacomm de México está interesado en implementar la norma ISO 27001 para ARCOM S.A pues reconocen la importancia de certificarse en esta norma pues es garantía del buen uso de las tecnologías de la información como también de que el personal está

capacitado para que la información tenga el menor grado de riesgo y este a salvo dando confianza y tranquilidad al cliente. Es por esto que General Datacomm de México está interesado en implementar dicha norma en el área de implementación de servicios y provisión, pues es el área que en los últimos meses mayor porcentaje de efectividad tiene, como se mira en la figura No.5, es por esto que la alta dirección considera que comenzar la implementación de esta norma en esta área es muy importante pues se maneja la información de los clientes de nuestro cliente principal y por ende el compromiso con la entrega y configuración de estos servicios corporativos es muy importante.

El compromiso de este proceso de certificación de la norma ISO 27001 no es solo de la alta dirección como tampoco del departamento de calidad quien se encarga de planear y ejecutar este proceso, es también compromiso de todos los ingenieros que conforman el área de implementación de servicios y provisión pues son los actores importantes en este proceso y gran parte de la obtención de esta certificación es por el trabajo, dedicación y compromiso que le impriman en la ejecución de este proceso.

Este proceso de certificación consiste en implementar políticas de seguridad en el uso de las tecnologías de la información, es por esto que el personal que compone el área de implementación de servicios y provisión deben identificar de manera general las vulnerabilidades y riesgos a la que la información está sometida, después de ser identificados el departamento de calidad establece políticas las cuales mitigan ese riesgo sugerido, identificado y reconocido por el departamento de calidad, la aplicación de dichas políticas es compromiso de área asumirlas, ejecutarlas y adaptar a la forma de trabajo del personal que integra el área, con esto la alta dirección quiere disminuir el riesgo de que la información sea violada, alterada, hurtada, modificada entre otros delitos informáticos.

General Datacomm de México y ARCOM S.A tienen el entusiasmo y total apoyo a el área de implementación de servicios y provisión para que este proceso que se comienza culmine con total éxito logrando implementar la costumbre de la seguridad de la información y con esto poder atraer más clientes con el fin de consolidarse como empresa de tercerización de servicios en Colombia y América Latina.

La generación de las políticas de seguridad en el proceso de implementación de la norma ISO 27001 estará a cargo del departamento de calidad encargado de implementar dichas políticas, estas serán implementadas de acuerdo a las amenazas y vulnerabilidades encontradas por el grupo, el departamento de calidad tiene en cuenta que el desarrollo de estas políticas debe estar alineadas con los objetivos principales de tanto de Datacomm como de ARCOM S.A

## **ALCANCES Y LIMITACIONES**

### **ALCANCES**

El área de provisión de ARCOM S.A es el área pionera en la empresa al certificar sus procesos bajo la norma ISO 27001 en un programa llevado por la alta dirección de la empresa en querer certificar sus procesos tanto en calidad ISO 9001, como en el buen uso de las Tecnologías de la Información TI ISO 20000, con esto ARCOM S.A estandariza todos sus procesos bajo normas internacionales.

El área de provisión es la encargada de configurar y dar soporte en la instalación de soluciones en telecomunicaciones al sector corporativo para la empresa Claro Soluciones Fijas antes conocida como Telmex S.A.

La dirección de ARCOM S.A está interesada en un primer momento por implementar en el área de Provisión la certificación de la norma ISO 27001, y luego con la obtención de las demás certificaciones anteriormente mencionadas implementar esta norma en los departamentos restantes los cuales están consignados en las características y composición de la empresa.

Es importante aclarar que para la dirección general es importante todas las dependencias de la empresa, pero en este proceso en la cual la empresa quiere certificarse en varias normas ISO/IEC/ICONTEC, el deseo de la dirección es la de empezar por esta área y

secuencialmente con la obtención de las demás certificaciones ir implementado la norma 27001 en las demás dependencias.

## **LIMITACIONES**

ARCOM S.A empresa con 5 años de experiencia en el sector de las Telecomunicaciones no tiene documentación suficiente en la cual estén registrados datos relevantes en el proceso de implementación de la norma ISO 27001, por ende esta información se debe ir levantando en el proceso que la implementación lo requiera.

ARCOM S.A al ser una empresa que presta servicios de tercerización la mayoría de los documentos que se requieren para documentar el proceso las tiene el cliente en este caso para el área de provisión la empresa a la que se le presta el servicio de tercerización de servicios es Claro Soluciones Fijas, y se depende de la gestión del cliente en la agilización en el trámite y acceso a dichos documentos.

## ENFOQUE HUMANÍSTICO

A lo largo del siglo XXI se ha notado una considerable evolución en el uso de las tecnologías de la información, la masificación del uso de computadores, teléfonos celulares inteligentes, tabletas y otros dispositivos como también el uso de redes de internet inalámbricas, además de que el acceso a estos dispositivos es cada mes más fácil pues entre las grandes empresas tanto desarrolladoras, fabricantes y prestadoras de productos y servicios en telecomunicaciones se han encontrado en disputa de patentes, servicios más económicos, ofrecer dispositivos de mejor calidad siempre a más bajo costo, donde el beneficiario siempre es el usuario.

La evolución en Colombia desde los últimos 10 años es evidente pues la tecnología que encontramos en dispositivos móviles en la actualidad es la misma con la que cuenta todo el mundo a diferencia de las redes en las cuales los dispositivos funcionan, con esto nos damos cuenta que lustros atrás el celular era un dispositivo con muchas limitación tanto en red como en funciones donde el costo por minuto era muy costoso y donde la cultura del teléfono fijo tenía una vigencia que al parecer no tenía caducidad. Ya haciendo un paralelo diez años después encontramos dispositivos móviles con muchas funciones y a un bajo costo donde las empresas prestadoras de telecomunicaciones brindan el mejor servicio en el soporte de estas redes y la mejora constantemente en ofrecer e innovar con novedosos servicios.

En la parte empresarial el cambio también fue significativo pues el uso de las redes tanto celulares como las de internet se fueron masificando pues la empresa vio en ellos un recurso eficiente y eficaz en el cual los recursos son notoriamente economizados y la información el activo más importante de una empresa además del recurso humano, se estaba siendo almacenados en lugares seguros. Pero con esto también surgió el delito informático, este que se conoce desde la segunda guerra mundial con la Maquina Enigma la cual fue usada para cifrar los mensajes y que el enemigo no pudiese tener acceso a dicha información, y que con

el tiempo se conoce como hacking<sup>12</sup>, las empresas siempre con la preocupación de que la información no esté en riesgo de ser alterada, hurtada o modificada se adapta a estándares internacionales los cuales no garantizan en un 100% pero si dependiendo de la disposición del personal a cargo de la información que este siempre a guardado.

En resumen el enfoque humanístico de esta monografía se basa en el personal participe en el proceso de implementación en la certificación de la norma ISO 27001, el proceso de certificación para cualquier empresa con cualquier objetivo empresarial en cualquier certificación a la cual quiera aplicar debe haber compromiso y participación de absolutamente todas las partes involucradas en el proceso, es con esto que el proceso humanístico es muy importante en este proceso pues no es solo ser el mejor profesional en cualquier campo laboral si no el de ser persona, tener compromiso basado en los principios tanto morales como éticos en la parte personal y laboral, pues se está confiando en estas personas información corporativa la cual en manos indebida puede ser de mucho riesgo para los intereses y el objetivo principal de la empresa.

El enfoque humanístico también se basa en la humanización de las Tecnologías de la Información pues el hecho de que la mayoría de los procesos y de medios de comunicación sean bajo la utilización de esta tecnología no significa con esto que la información que pierda su entorno humanístico del cual surge de la necesidad de una persona o un grupo de personas que conforman una sociedad, nos estamos dando cuenta que estas tecnologías invasivas hacen a una sociedad cada vez más permeada y más vulnerable al uso de estas tecnologías y esa brecha tecnológica de la cual somos partícipes, en la que el uso de dispositivos móviles hacen que perdamos el sentido de las relaciones sociales pues la segregación de la sociedad en su entorno se ve notablemente alterada.

---

<sup>12</sup>Termino Hacking definido como la delincuencia informática donde personas con avanzados conocimientos en informática busca como rompen esquemas de seguridad con el fin de acceder a información confidencial, esto basado en el libro Enredados el mundo de la internet por Alberto Villacorta

## **DELIMITACIÓN**

### **DELIMITACIÓN CRONOLÓGICA**

El desarrollo del proyecto se lleva a cabo de la siguiente manera:

Tabla No. 1 Cronograma de Actividades

<b>MES</b>	<b>ACTIVIDAD</b>
Noviembre	Recolección de la información
Diciembre	Análisis de la información y creación del texto.
Enero	Consolidación del texto y culminación del mismo.
Febrero	Entrega del texto final a la Facultad de Ingeniería de telecomunicaciones.

FUENTE: AUTOR

Complementando la información de la tabla No.1, al empezar las prácticas profesionales en ARCOM S.A, se hizo necesario buscar un problemática o temática que se pueda a tratar con el fin de empezar a desarrollar con el apoyo de los integrantes del arrea como también el apoyo del departamento de calidad quien mostro notable interés en el desarrollo de esta temática.

### **DELIMITACIÓN ESPACIAL**

La implementación de la norma ISO/IEC 27001 se llevara a cabo en el área de implementación y provisión de servicios ubicado en el edificio Nippon Center en la carrera 13ª No. 89-38 oficina 704, ubicado en la ciudad de Bogotá Distrito Capital, Colombia.

### **DELIMITACIÓN ECONÓMICA**

ARCOM S.A es consciente de la importancia de la implementación de la norma ISO/IEC 27001 es por esto que para el desarrollo de esta actividad se requiere de los siguientes implementos.

Tabla No. 2 Delimitación Económica

<b>ELEMENTO</b>	<b>REFERENCIA</b>	<b>PRECIO<sup>13</sup></b>
Computador Portátil	No aplica	\$1'000.000
Norma ISO/IEC 27001	NTC- ISO/IEC 27001. Tecnología de la Información. Técnicas De Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI).	\$45.000
Elementos de papelería	Esferas, lápices, papel bond, ganchos, carpetas, organizadores.	\$50.000
Impresora laser multifuncional	No aplica	\$200.000
Microsoft Office 2012	Programa licenciado para la realización de la documentación.	\$180.000

FUENTE; AUTOR

Los elementos anteriormente descritos son los que serán utilizados para el desarrollo de la actividad, en elementos como computador portátil e impresora láser multifuncional no aplican la referencia pues al ser un trabajo de documentación no necesita de requerimientos técnicos específicos por ende no se especifica referencia alguna o marca ya que no influyente para el desarrollo de la actividad.

## **METODOLOGÍA DE EVALUACIÓN DE RIESGOS**

El área de implementación de servicios y provisión recibe diariamente para los ingenieros puesta en marcha y para el ingeniero de configuración Ordenes de Trabajo (OT), estas

<sup>13</sup> Precios dados en pesos colombianos.

órdenes de trabajos se identifican con números aleatorios de siete dígitos, este número de orden de trabajo se consulta en el programa CRM (Control de Acceso Unificado) programa el cual tiene acceso tanto personal de ARCOM como personal de Claro soluciones fijas donde todo funcionario tiene su usuario y contraseña respectiva, donde están los datos tales como:

- Nombre del cliente
- Servicio a entregar o a configurar
- Ciudad en la que se ejecuta la actividad
- Información técnica del servicio a entregar
  - Nodo configurado
  - Puerto Lógico
  - Dirección IP
  - VLAN<sup>14</sup>
  - VRF<sup>15</sup>

Con estos datos se empieza la configuración o entrega de la instalación respectiva y debe ser documentada en la orden de trabajo, con la configuración y solución del servicio.

#### Medios de Transmisión

La información que se maneja para el área de implementación de servicios y provisión se manipula en el CRM como también en el programa 5620 SAM Client App cuyo fabricante es Alcatel Lucent, en el cual se tiene acceso y gestión a todas las redes con las que cuenta Claro Soluciones Fijas.

#### Destino y Origen de la información:

El origen de la información surge cuando el potencial cliente necesita una solución en telecomunicaciones, el ingeniero comercial es el encargado de analizar dicha necesidad del cliente y ofrecerle una solución al cliente.

---

<sup>14</sup>Virtual Local Network Area

<sup>15</sup>Virtual Routing Forwarding

El ingeniero Comercial se encarga de crear un número de Orden de Trabajo en el cual documenta:

- Nombre del cliente
- Solución requerida
- Condiciones eléctricas y físicas con las que cuenta la sede del cliente
- Contacto del cliente

Ya creada la orden de trabajo con los datos anteriormente mencionados pasa por el área de implementación en donde se realiza la topología de red para la entrega del servicio, configuración y entrega de servicios. Toda esta documentación generada durante el proceso de planificación, configuración e instalación de la solución debe ser documentada en el CRM (Control de Acceso Unificado), incluyendo correos electrónicos o registros de llamadas que se realizan para aclarar asuntos concernientes con la entrega del servicio con el fin de no tener inconvenientes con el cliente final. Ya cuando el servicio es entregado estas Ordenes de Trabajo son cerradas y no se le puede hacer modificación alguna, con esto se realiza un registro virtual de las actividades entregadas y la información pasa a ser almacenada en servidores con las que cuenta Claro Soluciones Fijas donde almacenan la información en bases de datos.

Identificación de riesgos y vulnerabilidades en el trayecto de la información:

- Para acceder al CRM (Control de Acceso Unificado), Claro Soluciones Fijas no habilita de manera inmediata nuevos usuarios para esta plataforma por lo que nuevo personal que ingrese al área de implementación de servicios y provisión deben utilizar usuarios y contraseñas de otros funcionarios del área, lo que significa un gran riesgo que significa poco control a quien accede a las información del cliente y no permite un registro adecuado de ingreso por usuario a dicha plataforma.
- En complemento los programas<sup>16</sup> de los diferentes fabricantes, no se cuenta con la licencia respectiva para cada funcionario y en algunos casos solo se tiene un usuario

---

<sup>16</sup>En el numeral 10. CONDICIONES FÍSICAS Y TÉCNICAS DEL ÁREA DE PROVISIÓN DE ARCOM S.A se especifica los programas utilizados, versiones y fabricante.

gestionado por programa, lo que implica un riesgo muy alto pues al iniciar de manera indebida la sesión y esta se bloquea se pierde gestión sobre el programa para toda el área lo que conlleva al retraso de las actividades hasta que Claro soluciones Fijas en el departamento de CORE pueda restablecer dicha sesión de usuario.

- Plataformas como CRM (Control de Acceso Unificado), 5620 SAM Client App son plataformas en las que frecuentemente se detectan problemas de conectividad pues son plataformas a la que ciento de personal tiene acceso y esta se satura por lo que en varias ocasiones los ingenieros del área de implementación de servicios y provisión no se pueden documentar acerca de la instalación que se va a llevar a cabo por lo que genera un retraso en la instalación del servicio y se afecta al cliente final con la entrega tardía del servicio.
- La información al ser transmitida por la red en su totalidad es vulnerable a ser permeada y modificada por medio de actividades delictivas electrónicas ya que si bien este programa y los usuarios que pueden acceder a esta base de datos son funcionarios de la empresa y de sus aliados, el ingreso indebido y el hurto de información puede darse de manera ilegal e indebida lo que hace la información vulnerable.

La implementación de la matriz de riesgos se llevará a cabo por medio de la clasificación de los activos, los integrantes del área de implementación de servicios y provisión de ARCOM S.A clasificaron los activos por ubicación, tipo de activo, formato, licencias, este se describe más a fondo el numeral 11.4 Inventario de Activos.

---

## INVENTARIO DE ACTIVOS

Identificación de activos dentro del alcance:

En el área de implementación de servicios y provisión los activos y los propietarios<sup>17</sup> de estos activos están asignado der la siguiente manera:

Tabla No.3 Inventario de activos área de implementación de servicios y provisión

Tipo de Activo	Formato	Ubicación	Información sobre soporte técnico	información de licencias
Computador HP 100	Equipo	Área de implementación de servicios y provisión	Departamento de Tecnologías de la Información ARCOM S.A	Departamento de Tecnologías de la Información ARCOM S.A
Teléfono CISCO 7960	Equipo	Área de implementación de servicios y provisión	Departamento de Tecnologías de la Información ARCOM S.A	Departamento de Tecnologías de la Información ARCOM S.A
Teléfono Nokia 2710	Equipo	Área de implementación de servicios y provisión	Departamento de Tecnologías de la Información ARCOM S.A	Departamento de Tecnologías de la Información ARCOM S.A

<sup>17</sup> Por propietario refiérase por los equipos y dispositivos móviles que se les asignan a cada uno de los funcionarios del área.

Orden de Trabajo	Programa	Computador HP 100	Departamento de CORE Claro Soluciones Fijas	Departamento de CORE Claro Soluciones Fijas
5620 SAM Client App	Programa	Computador HP 100	Departamento de CORE Claro Soluciones Fijas	Departamento de CORE Claro Soluciones Fijas
Control de Acceso Unificado	Programa	Computador HP 100	Departamento de CORE Claro Soluciones Fijas	Departamento de CORE Claro Soluciones Fijas
PuTTY Connection Manager	Programa	Computador HP 100	Departamento de CORE Claro Soluciones Fijas	Departamento de CORE Claro Soluciones Fijas
E managment	Programa	Computador HP 100	Departamento de CORE Claro Soluciones Fijas	Departamento de CORE Claro Soluciones Fijas
Local Maitenance Terminal	Programa	Computador HP 100	Departamento de CORE Claro Soluciones Fijas	Departamento de CORE Claro Soluciones Fijas
CISCO Unified CM Administration	Programa	Computador HP 100	Departamento de CORE Claro Soluciones Fijas	Departamento de CORE Claro Soluciones Fijas
TANDBERG	Programa	Computador HP 100	Departamento de CORE Claro Soluciones Fijas	Departamento de CORE Claro Soluciones Fijas

FUENTE: AUTOR

## **IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES**

Como se explica en la primera parte del texto las amenazas se clasifican en humanas y ambientales, para el área de implementación de servicios y provisión las amenazas y vulnerabilidades encontradas fueron:

### **Amenazas Ambientales:**

Para ARCOM S.A las amenazas ambientales constituye un tópico importante en la protección de sus empleados y de la información, es por esto que la compañía cuenta con políticas en la prevención del riesgo como también con elementos de primeros auxilios en el departamento de implementación de servicios y provisión, se cuentan con rutas de evacuación y en varias oportunidades en área y la empresa han participado en la realización de simulacros de emergencia esto con el fin de capacitar y concientizar al personal de la empresa en la gestión del riesgo.

Por parte de la información esta se encuentra en constante actualización por lo que se tienen servidores de respaldo donde se confina toda la información, para esto la alta gerencia a adecuado distintos puntos los cuales su ubicación es desconocida pues se ha determinado la rotunda confidencialidad de la ubicación de estos servidores de respaldo con el fin de que ante cualquier amenaza ambiental esta información este actualizada para documentaciones.

### **Amenazas Humanas:**

El área de implementación de servicios y provisión que cuenta con personal capacitado y en el área que responsable y eficaz en las labores asignadas y el cumplimiento de metas a coroto como largo plazo.

Como se ha anotado previamente el área de implementación de servicios y provisión y es la encargada de configurar e instalar servicios a clientes corporativos con los que cuenta Claro Soluciones Fijas, es por esto que la información de los clientes del cliente

principal de ARCOM S.A se ve afectada y las amenazas y vulnerabilidades encontradas son:

- Situaciones ajenas al personal de ARCOM S.A como hurto de los equipos, ingreso de personal que no pertenece al área de implementación de servicios y provisión como de otras dependencia, pues se está expuesto como cualquier otra edificación al hurto por parte de personas inescrupulosas que se encargan de saquear y hurtar edificaciones.
- Infiltración a las redes y servidores de ARCOM S.A por parte de delincuentes informáticos los cuales por medio de otras redes con solicitudes o en la búsqueda espacios en los cuales puedan permear y logren robar información valiosa para la empresa.

## **IDENTIFICAR IMPACTOS**

Es evidente que ante una emergencia de tipo ambiental el impacto es radical debido a que según el grado de gravedad es irreversible poder recuperar la información, algún evento de tipo sísmico, incendio, inundación, manifestaciones sociales entre otros eventos de tipo natural, para esto el impacto es máximo ya que no es posible determinar factores como el grado de afectación que pueda tener algún tipo de movimiento telúrico, como se puede controlar un incendio y que nivel de alcance tenga el mismo y cuáles fueron sus causas.

El hurto de activos físicos es sumamente grave debido a que en dichos dispositivos se encuentra toda la información de los diferentes clientes corporativos de Claro Soluciones fijas, como también usuarios y contraseñas de diferentes programas y bases de datos, información institucional de ARCOM S.A. entre otra tipo de información de carácter confidencial.

El ingreso no autorizado y forzado a las redes y servidores de ARCOM S.A constituye en un impacto crítico para la información de la empresa debido a que la mayoría de información es alojada en servidores ubicados en las sedes administrativas de la empresa, por lo que

cualquier infiltración, hurto, a dicha información constituye en un impacto crítico y grave para la empresa.

## ANÁLISIS Y EVALUACIÓN DE RIESGOS

Es importante identificar que amenazas y vulnerabilidades afectan directamente el objeto social de ARCOM S.A, debido a que ya siendo clasificadas estas amenazas y vulnerabilidades se pueden tratar de tres formas:

- **Asumir:** Los riesgos son asumidos directamente por ARCOM S.A cuando este afecta directamente con la línea de negocio de la empresa por lo que se le debe prestar mayor atención y por ende para el tratamiento de este riesgo se debe atención especial por parte de la alta gerencia y el departamento de calidad.
- **Mitigar:** Los riesgos se mitigan cuando las amenazas y vulnerabilidades afectan al objeto social y de negocio de ARCOM S.A pero su impacto no afecta de manera considerable el objeto de negocio, cuando se le aplica un control basado en la norma ISO 27001, y el riesgo residual es considerablemente bajo.
- **Transferir:** Los riesgos se transfieren cuando estos no están alineados con los objetivos de negocio de ARCOM S.A, por ende la alta gerencia y el departamento de calidad con el área de implementación de servicios y provisión determinan cuales de estos se transfieren y que empresa o persona natural está en la capacidad de asumirlo de manera efectiva.

En la tabla No. 2 CLASIFICACIÓN DE RIESGOS, se determina que riesgo, afectan directamente el objeto de negocio de la empresa y su forma de tratar el riesgo.

TABLA No. 4 Clasificación de riesgos

IDENTIFICACIÓN DEL RIESGO	TRATAMIENTO O DEL RIESGO	JUSTIFICACIÓN
Catástrofe ambiental	Mitigar	Por medio de campañas de reacción y prevención ante el desastre el departamento de gestión humana realiza

		campañas de concientización, actividades como simulacros y capacitación al personal de ARCOM S.A,
Infiltración a redes y servidores ARCOM S.A	Asumir	Es importante capacitar y contratar personal nuevo con conocimiento en la implementación y posterior administración de sistemas firewall para así poder controlar y monitorear los diferentes peticiones y requerimientos que se le haga a las redes de ARCOM S.A
Hurto y daños de las instalaciones	Transferir	El cuidado y control de entrada de a las oficinas de ARCOM S.A está a cargo de la administración y departamento de seguridad de Nippon Center quien se encargan de controlar el acceso del personal a las instalaciones como la de cuidar y vigilar las diferentes oficinas en horario no hábil.

FUENTE: AUTOR

Lo documentado en la tabla No.2 son los riesgo que se identificaron en el área de implementación de servicios y provisión en donde participa todos los funcionarios de dicho departamento con el área de calidad y la alta gerencia esto con el fin de que todos los entes interesados en este proceso de certificación, aporten de manera objetiva con el fin de que no se deje de lado ningún riesgo que pueda afectar los intereses de la empresa y se pueda salvaguardar la información que es lo que se busca proteger con la implementación de esta norma.

ARCOM S.A y el departamento de calidad tiene plena seguridad que el personal que labora en este departamento y que por más de 3 años ha consolidado un grupo humano y profesional que está interesado en la consolidación y evolución del área de implementación de servicios y provisión, por lo que no ve como una potencial amenaza el hurto de información por parte del personal que integra el área, pues durante el tiempo del área de implementación de servicios y provisión ha ejecutado actividades no se ha presentado el primer caso de hurto de información o de dispositivos físicos.

## **SELECCIÓN DE CONTROLES**

En la selección de controles se realizan teniendo en cuenta los riesgos documentados e identificados en la tabla No.2 CLASIFICACIÓN DE RIESGOS, basando se en la norma ISO 27001 del ICONTEC.

**RIESGO:** Catástrofe Ambiental.

**CONTROL:** Protección contra amenazas y externas y ambientales<sup>18</sup>

“Se deben diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial” (ICONTEC, 2006)<sup>19</sup>

**Implementación:**

El suministro de elementos de prevención tales como camilla, kit de primeros auxilios, extintor, inmovilizador de extremidades, los cuales en caso de emergencia están al alcance de los funcionarios.

Por otra parte el departamento de gestión humana capacita al personal del área de implementación y provisión de servicios en temas como reacción ante el riesgo, conformando brigadas internas donde en estos casos se capacitan en cómo actuar en el momento.

---

<sup>18</sup> Basado en el numeral A.9.1.4 Protección contra amenazas y externas y ambientales del anexo A OBJETIVO DE CONTROL Y CONTROLES, NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

<sup>19</sup> numeral A.9.1.4 Protección contra amenazas y externas y ambientales del anexo A OBJETIVO DE CONTROL Y CONTROLES, NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001 JUNIO 2006

**RIESGO: INFILTRACIÓN A REDES Y SERVIDORES ARCOM S.A**

**CONTROL:** Gestión de la seguridad de las redes<sup>20</sup>

“Asegurar la protección de la información en las redes y protección de la infraestructura de soporte. La gestión segura de las redes, las cuales pueden sobrepasar las fronteras de la organización, exigen la consideración cuidadosa del flujo de datos, las implicaciones legales, el monitoreo y protección” (ICONTEC, 2006)<sup>21</sup>

**Implementación:**

La capacitación y contratación de personal con experiencia en la implementación y posterior monitoreo en plataformas de seguridad tales como servidores firewall y servidores de redes privadas virtuales, plataformas las cuales deben monitorear registros de direcciones IP donde se registre las solicitudes, tiempo y hora de la solicitud, como también los puertos y protocolos por los cuales se están estableciendo dichas solicitudes

**RIESGO: HURTO Y DAÑO DE LAS INSTALACIONES**

**CONTROL:** Seguridad de Oficinas, Recintos e Instalaciones<sup>22</sup>

“Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones” (ICONTEC, 2006)<sup>23</sup>

---

<sup>20</sup> Basado en el numeral A.10.6 gestión de la seguridad de las redes del anexo A OBJETIVO DE CONTROL Y CONTROLES, NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

<sup>21</sup> numeral A.10.6 Gestión de la seguridad de las redes del anexo A OBJETIVO DE CONTROL Y CONTROLES, NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001 JUNIO 2006

<sup>22</sup> Basado en el numeral A.9.1.3 Seguridad de Oficinas, Recintos e Instalaciones del anexo A OBJETIVO DE CONTROL Y CONTROLES, NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

<sup>23</sup> numeral A.9.1.3 Seguridad de Oficinas, Recintos e Instalaciones del anexo A OBJETIVO DE CONTROL Y CONTROLES, NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001 JUNIO 2006

**Implementación:**

Para el ingreso a las oficinas de ARCOM S.A se deben ser anunciados a la recepción de ARCOM S.A para el ingreso a las instalaciones de la empresa, para el personal del área de implementación de servicios y provisión y demás funcionarios se les asigna una tarjeta inteligente la cual monitorea el ingreso y la salida de los funcionarios, para la seguridad de las oficinas se cuenta con la supervisión del departamento de seguridad con la que cuenta el edificio Nippon Center quien deben estar vigilando contantemente dichas instalaciones.

## CONCLUSIONES

La implementación de la norma técnica ISO 27001 es aplicable en cualquier entorno laboral donde se quieran mejorar las prácticas en el manejo de tecnologías de la información, debido a que en la actualidad la información ya dejó de ser netamente documentada por el contrario ahora la información es manejada virtualmente, almacenada en servidores dedicados y se puede consultar de manera segura como el uso de intranet o servidores por medio de protocolos de transferencia.

La participación del personal involucrado en procesos de certificación es vital, debido a que ellos son los encargados de aplicarlas y de manipular de forma correcta la información, en el proceso de implementación de la norma es necesario el trabajo en conjunto con el personal de calidad que esté llevando el proceso, es por esto que los más interesados en la aplicación de la norma son el personal del área quienes son los directamente beneficiados en dicho proceso.

En el caso de ARCOM S.A una empresa dedicada a la tercerización de servicios se hace un poco más complejo la aplicación de la norma debido a que en el caso de los programas de gestión y configuración de redes se hace más difícil que los clientes respondan los requisitos de manera ágil y eficiente lo cual entorpece un poco la implementación de la norma.

El reconocimiento de amenazas y vulnerabilidades en el área de implementación de servicios y provisión se torna en algunos momentos subjetiva debido que algunos tópicos en los cuales para el área de seguridad es crítico y merece de especial apoyo por parte de provisión, el personal de implementación de servicios no le ven la criticidad ya indicada, es por eso que algunas amenazas y vulnerabilidades no quedaron registrados en el proyecto.

El proceso de certificación de la norma ISO 27001, tiene una especial afinidad con la ingeniería de telecomunicaciones pues se implementan y se generan procesos los cuales en el área son recientes y que abarcan una gran cantidad de información y conocimientos que

en el oficio de la ingeniería de telecomunicaciones es un complemento vital en el proceso de ser profesional integral.

La aplicación de esta norma técnica en empresas que quieran controlar y mejorar el uso de las tecnologías de información, humaniza un poco el uso de las tecnologías debido a que por medio de estas estructuras estamos conociendo y tomando controles los cuales promueven la seguridad de la información.

El proceso de certificación es un proceso en el cual muchas dependencias de la empresa se unen por un bien común, lo cual en el ámbito laboral y humano estrecha y fortalece las relaciones interpersonales de los funcionarios lo cual mejora notablemente el ámbito laboral, social y personal.

La consecución de la norma ISO 27001 es un logro de todo el personal involucrado en dicho proceso, lo que refleja la importancia del trabajo en grupo donde todos hacen pieza importante en el proceso de certificación lo cual fortalece e impulsa a trabajar por un proyecto que es reconocido a nivel internacional

## **BIBLIOGRAFÍA**

*MANIK DEY (2007). I Management Information Security: IEEE*

*INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACION  
ICONTEC. (2007), Norma Técnica NTC – ISO/IEC 27001*

*FERRER, RODRIGO (2008), Metodología de análisis de riesgo*

*FERRER, RODRIGO (2008), Sistema de gestión de seguridad de la información SGSI.*

*POVEDA JOSE MANUEL (2010), Definición de las políticas, organización, alcance  
del sistema de gestión y concienciación.*