RESUMEN – TRABAJO DE GRADO

AUTORES	GINA FERNANDA ALVAREZ MUÑOZ JUAIS CELEDON ALARCON OBER ALFREDO RUIZ DAZA
FACULTAD	FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS	ESPECIALIZACION EN AUDITORIA DE SISTEMAS
DIRECTOR	YESICA MARIA PEREZ PEREZ
TÍTULO DE LA TESIS	GUÍA DE GESTIÓN DE RIESGOS TECNOLÓGICOS PARA EL PROCESO DE CONSULTA EXTERNA DE LA IPS DR PROSALUD S.A.S OCAÑA, N. DE S.

RESUMEN

(70 palabras aproximadamente)

LA INFORMACIÓN ES EL ACTIVO MÁS IMPORTANTE DE UNA ORGANIZACIÓN, EL CUAL TIENE TRES CARACTERÍSTICAS IMPORTANTES: LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD. DICHAS CARACTERÍSTICAS PUEDEN SER AFECTADAS POR CUALQUIER INCIDENTE DE LOS MENCIONADOS ANTERIORMENTE Y APLICA TANTO PARA LA INFORMACIÓN ALMACENADA EN MEDIOS MAGNÉTICOS COMO DE FORMA FÍSICA. SIN EMBARGO, NO ES EL ÚNICO ACTIVO QUE PUEDE SER AFECTADO YA QUE TAMBIÉN LOS ACTIVOS FÍSICOS COMO RECURSOS TECNOLÓGICOS Y CENTROS DE OPERACIÓN ENTRE OTROS.

CARACTERÍSTICAS

PÁGINAS:95	PLANOS:	ILUSTRACIONES: 5	CD-ROM: 1

GUÍA DE GESTIÓN DE RIESGOS TECNOLÓGICOS PARA EL PROCESO DE CONSULTA EXTERNA DE LA IPS DR PROSALUD S.A.S OCAÑA, N. DE S.

GINA FERNANDA ALVAREZ MUÑOZ
JUAIS CELEDON ALARCON
OBER ALFREDO RUIZ DAZA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
2016

GUÍA DE GESTIÓN DE RIESGOS TECNOLÓGICOS PARA EL PROCESO DE CONSULTA EXTERNA DE LA IPS DR PROSALUD S.A.S OCAÑA, N. DE S.

GINA FERNANDA ALVAREZ MUÑOZ
JUAIS CELEDON ALARCON
OBER ALFREDO RUIZ DAZA

Trabajo de grado para optar el título de Especialista en Auditoría de Sistemas

Directora
YESICA MARIA PEREZ PEREZ
MDE(C).ESP. Ingenieria De Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
FACULTAD DE INGENIERIAS
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
2016

DEDICATORIA

A Dios, por permitirme llegar a este momento tan especial, por los triunfos y los momentos difíciles que me han enseñado a valorar cada día más. A mis padres, en especial a mi madre LUISA ALARCÓN GUERRA que con su apoyo incondicional me da fuerzas y me acompaña siempre con sus oraciones. A mi esposa YEINY ARENAS RODRIGUEZ y mi linda hija LUCIANA CELEDÓN ARENAS quien es mi motor, la dueña de todo por lo que lucho. A mis profesores que guiaron y apoyaron en este proceso de formación. A mis compañeros Gina y Ober que sin ellos, esto no podría haberse materializado.

Gracias a todos.

A Dios por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos. A mis padres por ser el pilar fundamental en todo lo que soy, por su apoyo mantenido a través del tiempo. A mi hermano por estar siempre presente acompañandome para poderme realizar. A los docentes y compañeros por acompañarme, guiarme y brindarme su apoyo en este proceso. A mi esposo Ober Alfredo por estar conmigo en aquellos momentos en que el estudio y el trabajo ocuparon mi tiempo y esfuerzo. Gracias por toda tu ayuda.

GINA FERNANDA ALVAREZ MUÑOZ

A Dios quién sabe guiarme por el buen camino en todo momento. A mis padres y hermanos quienes por ellos soy lo que soy. A mi adorada esposa Gina Fernanda por ser mi mayor bendición y el horizonte de mi vida en todo momento para alcanzar nuevas metas, tanto profesionales como personales.

OBER ALFREDO RUIZ DAZA

AGRADECIMIENTOS

Queremos agradecerles a cada una de las personas que nos colaboraron en la realización de este proyecto; a las directivas de la IPS Dr. Prosalud S.A.S. por facilitarnos las instalaciones de su organización para el desarrollo de cada una de las actividades realizadas en el proyecto de investigación.

A nuestra directora del proyecto de investigación MDE. Yesica Maria Perez Perez, por su empeño, dedicación y seguimiento durante todo este proceso.

A cada uno de los docentes que durante el proceso en la especialización aportaron su conocimiento para nuestra formación profesional.

TABLA DE CONTENIDO

pág.

INTRODUCCION 12

1. TITULO 13
1.1 PLANTEAMIENTO DEL PROBLEMA 13
1.2 FORMULACIÓN DEL PROBLEMA 13
1.3 OBJETIVOS 13
1.3.1 General 13
1.3.2 Específicos 14
1.4 JUSTIFICACIÓN 15
1.5 HIPÓTESIS 15
1.6 DELIMITACIONES 15
1.6.1 Geográfica 15
1.6.2 Temporal 16
1.6.3 Conceptual 16
1.6.4 Operativa 16

2. MARCO REFERENCIAL 17
2.1 MARCO HISTÓRICO 17
2.1.1 Antecedentes. 18
2.2 MARCO CONCEPTUAL 18
2.3 MARCO TEÓRICO 21
2.4 MARCO LEGAL 24

3. DISEÑO METODOLÓGICO 25
3.1 TIPO DE INVESTIGACIÓN 25
3.2 POBLACIÓN Y MUESTRA 25
3.3 TECNICAS E INTRUMENTOS 25

4. PRESENTACION DE RESULTADOS 27
4.1 MODELO DEL NEGOCIO DEL PROCESO DE CONSULTA EXTERNA DE LA IPS DR PROSALUD S.A.S. 27
4.1.1 Misión y Visión de la IPS Dr. Prosalud S.A.S. 27
4.1.2 Objetivos Organizacionales de la IPS Dr. Prosalud S.A.S. 27
4.1.3 Principios y Valores Corporativos de la IPS Dr Prosalud S.A.S. 28
4.1.4 Estructura Orgánica de la IPS Dr Prosalud S.A.S. 28
4.1.5. Mapa de Procesos de la IPS Dr Prosalud S.A.S. 29
4.1.6 Cadena de Valor de la dependencia Consulta Externa 30
4.1.7 Procesos y Subprocesos de la dependencia Consulta Externa 31
4.1.8 Modelo de Actores de la IPS DR. Prosalud S.A.S. 40
4.1.9 Infraestructura tecnología 42
4.2 ESTADO ACTUAL DEL PROCESO DE CONSULTA EXTERNA DE LA IPS 45

DR PROSALUD S.A.S. POR MEDIO DE UNA AUDITORIA PASIVA BASADA EN NTC-ISO-IEC-27001
4.2.1 Presentación del grupo auditor 45
4.2.2 Programa de auditoria 46
4.2.3 Guía de auditoria 49
4.2.4 Inventario de software 51
4.2.5 Inventario de Hardware 52
4.2.6 Desviaciones encontradas 53
4.2.7 Situaciones encontradas 54
4.2.8 Situaciones relevantes 56
4.2.9 Pruebas y resultados 57
4.2.10 Dictamen 63
4.2.11 Evaluación de Controles al proceso de Consulta Externa de la IPS Dr. Prosalud S.A.S. basada en NTC-ISO-IEC-27001 64
4.3 GUÍA DE GESTIÓN DE RIESGOS COMO APOYO A LA SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE CONSULTA EXTERNA DE LA IPS DR PROSALUD S.A.S 65
4.3.1 Proposito de la guía de gestión de riesgos. 65
4.3.2 Alcance de la guía de gestión de riesgos. 65
4.3.3 Usuarios de la guía de gestión de riesgos 65
4.3.4 Objetivo de la guía de gestión de riesgos. 65
4.3.5 Guía de Aplicación de la norma 65
4.3.6 Valoración del riesgo 67
4.3.6.1 Monitoreo y revisión 78

CONCLUSIONES 79

RECOMENDACIONES 80

BIBLIOGRAFIA 81

REFERENCIAS DOCUMENTALES ELECTRONICAS 82

ANEXOS 84

LISTA DE FIGURAS

pág.

Figura 1. Organigrama 19
Figura 2. Valores Corporativos de la IPS Dr Prosalud S.A.S. 28
Figura 3. Organigrama de la IPS Dr. Prosalud S.A.S. 29
Figura 4. Mapa de Procesos de la IPS Dr. Prosalud S.A.S. 30
Figura 5. Cadena de de la IPS Dr. Prosalud S.A.S. 31
Figura 6. Proceso Medicina General de la IPS DR Prosalud S.A.S 32
Figura 7. Subprocesos Medicina General de la IPS DR Prosalud S.A.S 33
Figura 8. Subprocesos de Generación de Citas de la IPS DR Prosalud S.A.S 34
Figura 9. Subprocesos de Consulta Externa de la IPS DR Prosalud S.A.S 35
Figura 10. Subprocesos de Facturación y Cobro de la IPS DR Prosalud S.A.S 36
Figura 11. Proceso Odontología de la IPS DR Prosalud S.A.S 37
Figura 12. Subproceso Odontología de la IPS DR Prosalud S.A.S 38
Figura 13. Subprocesos de Generación de Citas de la IPS DR Prosalud S.A.S 38
Figura 14.Subprocesos de Consulta Externa de la IPS DR Prosalud S.A.S 39
Figura 15. Subprocesos de Facturacion y Cobro de la IPS DR Prosalud S.A.S 40

LISTA DE CUADROS

Pág.

Cuadro 1. Objetivos y actividades 14
Cuadro 2. Planeación 19
Cuadro 2. Objetivos y actividades 25

INTRODUCCION

Todas las actividades relacionadas con la tecnología de una organización deben planificarse a lo largo del tiempo, teniendo en cuenta que el activo más importante en una organización son los datos, y que de ellos se debe tener en los niveles más altos la confidencialidad, la integridad y la disponibilidad, dichas características pueden ser afectadas por muchos factores que deben ser tenidos en cuenta para tratar de mitigar el riesgo inherente a ellos. En algunas organizaciones basan su seguridad e integridad de la información sólo a dispositivos físicos, redes, unidades de almacenamiento y software dejando de lado el acceso físico del personal que ingresa a la organización y las condiciones ambientales de los sitios donde reposa la información.

En el momento que la organización ve la necesidad de implementar un plan de riesgos tecnológico, lo que implica la identificación y secuencia de las actividades, la asignación de recursos humanos, tecnológicos, económicos y métodos de control del progreso de las actividades, la planificación debe realizarse teniendo en cuenta todo lo que puede suceder en consecuencia con lo que se ha pensado y valorado.

En el área de consulta externa de la IPS Dr Prosalud S.A.S. se concentran todas las actividades relacionadas con el flujo de información la cual está siempre expuesta a la pérdida, retardo y manipulación causando inconformismo con los clientes y conflictos legales que se convierten en un derroche de recursos económicos.

Una manera de asegurar que los procesos se lleven a cabo en completa normalidad es el establecimiento de una guía de gestión de riesgos tecnológicos que permitan crear las normas a seguir para la protección de la integridad, confidencialidad y disponibilidad de la información.

En la presente investigación se realizó el diseño de una guía de gestión de riesgos tecnológicos para el proceso de consulta externa de la IPS Dr Prosalud S.A.S Ocaña, N. de S. siguiendo una metodología con miras a la mejora continua, donde en un inicio se efectuó el análisis de la situación actual de la IPS Dr Prosalud S.A.S en materia de seguridad para esto se contó con técnicas de recolección de información como encuestas, análisis y evaluación de riesgos y auditorias.

Teniendo identificado los riesgos asociados al proceso de consulta externa de la IPS Dr Prosalud S.A.S. se procedió a revisar las diferentes herramientas de auditoría para aplicar la que se mejor se adaptara y así empezar a generar la guía de gestión de riesgos tecnológicos, luego de documentar todo el proceso donde se evidencia el seguimiento de las buenas practicas asociadas a la gestión de riesgos y por último se pone en práctica la guía de gestión de riesgos tecnológicos para la IPS Dr Prosalud S.A.S. basados en la norma ISO 31000-2009 probando su efectividad al momento de mitigar los riesgos asociados al proceso de consulta externa de ésta institución preservando los principios básicos de la información.

1. TITULO

GUÍA DE GESTIÓN DE RIESGOS TECNOLÓGICOS PARA EL PROCESO DE CONSULTA EXTERNA DE LA IPS DR PROSALUD S.A.S OCAÑA, N. DE S.

1.1 PLANTEAMIENTO DEL PROBLEMA

La información es el activo más importante de una organización, el cual tiene tres características importantes: la confidencialidad, la integridad y la disponibilidad[1]. Dichas características pueden ser afectadas por cualquier incidente de los mencionados anteriormente y aplica tanto para la información almacenada en medios magnéticos como de forma física. Sin embargo, no es el único activo que puede ser afectado ya que también los activos físicos como recursos tecnológicos y centros de operación entre otros

El área de Consulta Externa de la IPS Dr Prosalud S.A.S. es la dependencia encargada de registrar, almacenar y actualizar los registros de los pacientes.

En la IPS Dr Prosalud S.A.S se viene presentando inconsistencias en el manejo de la información exponiéndola a la pérdida, retardo y manipulación de la información generando inconvenientes legales e inconformismo en los clientes afectando la imagen corporativa.

Así mismo, la información que procesa la IPS Dr Prosalud S.A.S. posee un alto grado de sensibilidad en cada uno de sus procesos y está expuesta permanentemente a riesgos que comprometen su disponibilidad, integridad y confidencialidad.

1.2 FORMULACIÓN DEL PROBLEMA

El desarrollo de este trabajo de investigación se fundamenta en ¿Cómo una guía de gestión de riesgos tecnológicos en la IPS Dr Prosalud S.A.S. permitirá la identificación y mitigación de riesgos?

1.3 OBJETIVOS

1.3.1 General

Diseñar una guía de gestión de riesgos tecnológicos en la IPS Dr Prosalud S.A.S.; Ocaña, N. de S. en el proceso de Consulta Externa que permita una mayor seguridad de la información.

[1] G. Granados Paredes, «Introducción a la criptogragía,» Revista Digital Universitaria, vol. 7, nº 7, pp. 2-17, 2006.

1.3.2 Específicos

Diseñar el Modelo del Negocio del proceso de Consulta Externa de la IPS Dr Prosalud S.A.S.

Diagnosticar el estado actual del proceso de Consulta Externa de la IPS Dr Prosalud S.A.S. por medio de una auditoria pasiva basada en NTC-ISO-IEC-27001

Crear una guía de gestión de riesgos como apoyo a la seguridad de la información para el proceso de Consulta Externa de la IPS Dr Prosalud S.A.S..

Cuadro 1. Objetivos y actividades

Objetivo específico	Actividades	Entregable
Diseñar el Modelo del Negocio del proceso de Consulta Externa de la IPS Dr Prosalud S.A.S.	Realizar visita a la IPS Dr Prosalud para identificar los procesos de la empresa	Modelo del Negocio
	Identificar el Mapa de Procesos	
	Identificar los procesos y subprocesos de apoyo.	
	Identificar la infraestructura tecnológica de la IPS Dr. Prosalud S.A.	
Diagnosticar el estado actual del proceso de Consulta Externa de la IPS Dr Prosalud S.A.S. por medio de una auditoria pasiva basada en NTC-ISO-IEC-27001	Elaborar instrumentos de recolección de información	Informe auditoria pasiva basada en NTC-ISO-IEC-27001
	Aplicar los instrumentos de recolección de la información en la IPS Dr. Prosalud S.A.	
	Análisis de los resultados obtenidos en la aplicación de instrumentos de recolección de información	Dictamen de la auditoria
	Realizar búsqueda documental para dar soporte a la auditoria	
Crear una guía de gestión de riesgos como apoyo a la seguridad de la información para el proceso de Consulta Externa de la IPS Dr Prosalud S.A.S..	Realizar un análisis de las metodologías de gestión de riesgos actuales.	Guía de Gestión de Riesgos para el proceso de Consulta Externa de la IPS Dr Prosalud S.A.S.
	Seleccionar la metodología de gestión de riesgos que se adapta al proceso de la IPS	

	Dr Prosalud S.A.S.	
	Realizar una guía de Gestión de riesgos para el proceso de Consulta Externa de la IPS Dr Prosalud S.A.S.	

Fuente: Autores del Proyecto

1.4 JUSTIFICACIÓN

Las organizaciones de todo tipo y tamaño enfrentan factores e influencias, internas y externas, que crean incertidumbre sobre si ellas lograrán o no sus objetivos. El efecto que esta incertidumbre tiene en los objetivos de una organización es el riesgo"[2].

La gestión de riesgos consiste en detectar los posibles peligros a los que está expuesta la empresa y adoptar las medidas oportunas. Se trata de tener la situación controlada "planificando la imprevisibilidad" con el fin de reaccionar con rapidez en caso de que surjan imprevistos, así como de mantener una ventaja competitiva.[3]

Actualmente en la IPS Dr Prosalud S.A.S. no existe implementado alguna norma basada en gestión de riesgos por lo tanto la información está expuesta a perdidas afectando la integridad, confidencialidad y disponibilidad de la misma y de esta forma se afectando los objetivos misionales de la empresa

Una guía de gestión de riesgos para la IPS Dr Prosalud S.A.S. es importante ya que permite identificar amenazas, debilidades que se convertirán en oportunidades de mejora y mitigar riesgos que ocasionen perdidas de información.

1.5 HIPÓTESIS

Una guía de gestión de riesgos en el proceso de Consulta Externa de la IPS Dr Prosalud S.A.S. contribuirá a la protección y creará valor dentro de la IPS para alcanzar los objetivos propuestos y mejorar su competitividad. El beneficio de realizar una gestión continua de estos riesgos es la de trabajar de manera oportuna para evitar que esas amenazas se concreten y eviten el cumplimiento de los objetivos y/o generen sobrecostos.

[2] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del Riesgo. Principios y Directrices. Bogotá D.C.: ICONTEC, 2011.NTC ISO 31000.

[3] Expense Reduction Analyst. Gestion de riesgos en la empresa. [En linea]. Publicado en internet en el año (2009-2016). Ubicado en la URL: http://expensereduction.eu/es/blog/gesti%C3%B3n-de-riesgos-en-la-empresa#.VhRx7_l_Oko

1.6 DELIMITACIONES

1.6.1 Geográfica

Este proyecto se desarrollará en el proceso de Consulta Externa de la IPS Dr Prosalud S.A.S., Ocaña, N. de S.

1.6.2 Temporal

El periodo de realización de la investigación será de tres (3) meses a partir de la aprobación del proyecto

1.6.3 Conceptual

Los conceptos que abarcarán esta investigación se fundamenta en gobernabilidad de TI y seguridad de la información, específicamente relacionados con la administración de riesgos y buenas prácticas.

NTC ISO/IEC 27001 Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI). 2005.

NTC ISO/IEC 27002 Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. 2005.

NTC 5254. Gestión del Riesgo. 2004.

NTC ISO/IEC 27005. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información. 27005.

NTC ISO 31000. Gestión del Riesgo. Principios y Directrices. 2011

PMBOK. Guía de los Fundamentos para la Dirección de Proyectos. 2008.

1.6.4 Operativa

La investigación del proyecto desde el punto de vista operativo se basa en los procesos que hacen parte Consulta Externa en la IPS Dr Prosalud S.A.S

Medicina General

Odontología

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

El manejo de la información hace años en las organizaciones pasaba desapercibida, siendo considerada como un elemento más en el desarrollo de sus procesos y operaciones. Con el paso del tiempo, debido a la incorporación de la tecnología y los grandes avances tecnológicos en cuanto a hardware, software, telecomunicaciones y la interacción que tiene el hombre con estas herramientas, la cual son utilizadas para almacenar, procesar, generar y transportar la información así como ha logrado facilitar el desarrollo operativo de las empresas, igualmente, como consecuencia de su devastada cantidad de información soportada en estos medios y en el ser humano, incrementa las posibilidad de que se encuentre en riesgo y sea atacada por amenazas informáticas que pueden causar impacto en el negocio. Por tal razón, hoy en día la seguridad de la información se ha convertido en un tema de vital importancia para las organizaciones.

La información actualmente es considerada un activo que representa gran valor para cualquier organización. Por tal motivo, se hace necesario protegerla y darle un manejo adecuado a la misma con el fin de evitar impactos significativos que pueden ser causados por agentes externos o interno que permanentemente se encuentran a esperas para aprovechar las vulnerabilidades o puntos débiles que presentan los sistemas de información en las organizaciones. Cabe aclarar, que los sistemas de información están compuestos por activos que cumplen funciones dentro de los mismos. Estos activos son las personas, el hardware, el software, los procesos, la infraestructura y la misma información, entre otros. Para este proyecto se consideran activos de información los mencionados anteriormente. Dichos activos están sujetos a ser atacados por amenazas que de no controlarse pueden causar impactos en la información y en efecto a la organización reflejándose en pérdidas económicas y de imagen. Así de esta manera, la alta dirección de cualquier organización debe ser consciente de que su información siempre se encontrará en riesgo y que debe tomar las medidas necesarias para enfrentarse a este tipo de adversidades.[4]

Hablar de seguridad de la información involucra muchos conceptos en especial el delo que significa el riesgo de TI y la manera de administrarlo o gestionarlo en la organización. Existen muchos estudios donde se aplican los conceptos de gestión de riesgos de tecnologías de la información en las organizaciones. Se habla de procesos, metodologías, planes tratamiento, mapas de riesgo, herramientas tecnológicas para riesgos. Pero, aún es muy ambiguo el concepto de modelo de gestión para manejar los riesgos de TI. Siendo esta una temática que trae consigo ser la razón fundamental o el motor que hace parte de un gran Sistema de Gestión de Seguridad de la Información, o comúnmente llamado SGSI. Un

[4] ACOSTA PORTILLO. Dinael, ALVAREZ PRADA. Ingrid Lorena, CAMARGO BARBOSA. Jorge Alberto, NÚÑEZ ASCANIO. Karen Lorena. Diseño de un modelo de gestión del riesgo de tecnologías de información para la unidad de contabilidad de la universidad francisco de paula Santander [Libro]. - OCAÑA : Tesis de grado para la Esp Auditoria de Sistemas, 2013.

SGSI debe gestionar el riesgo a través de la definición e implementación de elementos y prácticas que garanticen proteger la información.

2.1.1 Antecedentes. Para el desarrollo de esta propuesta se tuvieron en cuenta los siguientes antecedentes:

Diseño de una Política de Gestión de Riesgos de la Información para La Dependencia de Admisiones Registro y Control de Universidad Francisco de Paula Santander Ocaña. Autor: Yenis Piedad Osorio Rivero, Yesica María Pérez Pérez; 2014. Este proyecto nos sirve de referencia para determinar la mejor practica en la realización de la guía de gestión de riesgos ya que en su documento se sustenta en el marco de trabajo de ISO/IEC 31000/ 2009 y en la metodología de análisis y gestión de riesgos de los sistemas de información Magerit.[5]

Análisis de evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la alcaldía de pamplona - Norte de Santander, Autor: Jorge Enrique Ramírez Muñoz. 2015. Este proyecto sirve de referencia en la investigación ya que realiza un análisis y evaluación de riesgos para asesorar e implementar mejoras en la seguridad informática de un área específica.[6]

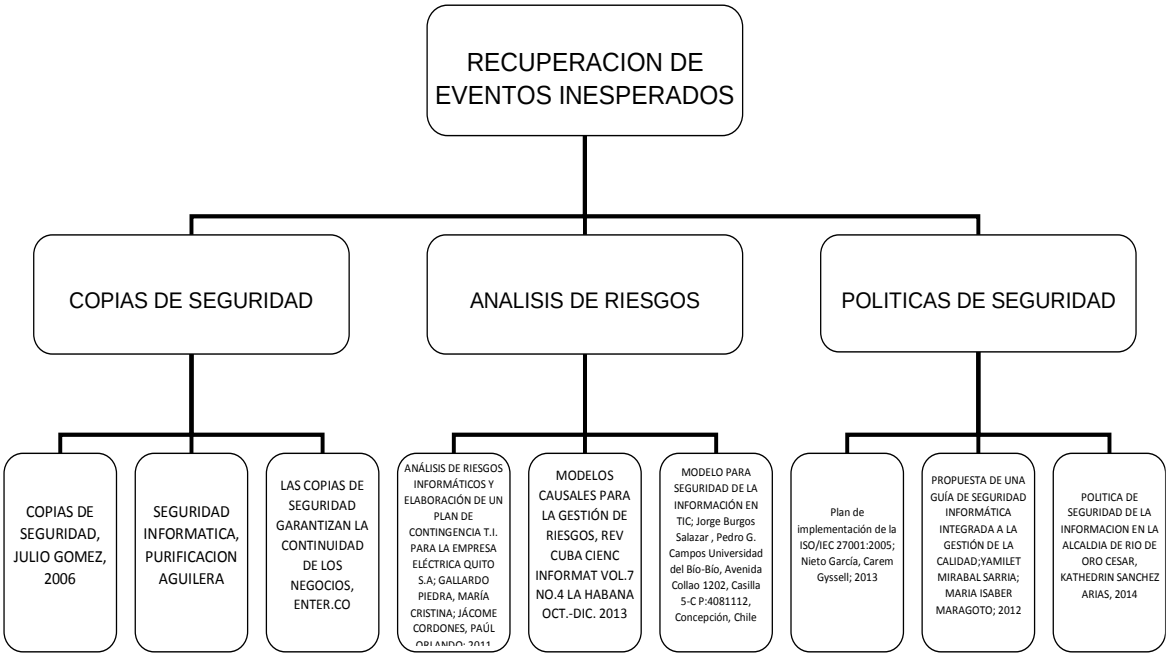
2.2 MARCO CONCEPTUAL

Teniendo en cuenta, que la presente propuesta está enfocada en la gestión de riesgos de la información, también se involucran conceptos relacionados con Seguridad de la Información que consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

[5] OSORIO RIVERO. Yenis piedad, PÉREZ PÉREZ. Yesica maría. Diseño de una política de gestión de riesgos de la información para la dependencia de admisiones registro y control de universidad francisco de paula Santander Ocaña. Autor: Tesis de grado para la Esp Auditoria de Sistemas, 2014

[6] RAMIREZ MONTAÑEZ. Jorge enrique. Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la alcaldía de pamplona - norte de Santander. [En línea]. Publicado en internet en el año 2015. Ubicado en la URL: http://hdl.handle.net/10596/3415 http://repository.unad.edu.co/handle/10596/3415

Figura 1. Mapa conceptual de investigación



Fuente: Autores del proyecto

Cuadro 2. Planeación

PLANEACION			BUSQUEDA Y CAPTACION
TEMA	**SUBTEMA**	**DESGLOSE SUBTEMAS**	**OPERADORES BOOLEANOS UTILIZAR**
Recuperacion de eventos inesperados	Copias de seguridad	Espacio	AND , " ", ;
		Dispositivo	**COMBINACION DE PALABRAS CON LOS OPERADORES BOOLEANOS**
		Salvaguarda	"Análisis de Riesgos" and "Seguridad de la Informacion",
	Analisis de riesgos	S.I.	"Análisis de Riesgos" and "politica de seguridad" and "ti",
		Riesgo	**MOTORES DE BUSQUEDA A UTILIZAR**
		Control	Eumed, Google Academico, Repositorio de Universidad Nacional
		Vulnerabilidad	
		Impacto	
		Amenaza	
	Politicas de seguridad	Normas de S.I.	
		Calidad de S.I.	
ANALISIS DE INFORMACION			**RESULTADOS Y CONCLUSIONES**
PRINCIPALES IDEAS ENCONTRADAS			
1. Las amenazas que pasan sobre la empresa son de naturaleza multiple y en constante evaluacion. 2. Antes de implementar una politica de seguridad es indispensable saber el nivel de seguridad que necesitamos. 3. Identificar cuál es la metodología de análisis de riesgos que proporciona una mejor oportunidad de toma de decisiones dentro de una organización frente a la custodia de la información, la cual se ha convertido en uno de los activos más importantes del ámbito empresarial e implica una adecuada utilización y preservación para garantizar la seguridad y la continuidad del negocio.			**¿QUÉ SE DESCUBRIO?** Existen varias metodologias para realizar el analisis y gestion de riesgos **¿QUÉ SE CONOCIO?** Metodologias para el analisis de riesgos OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS, NIST SP 800:30. **COMO APORTA A LA SOLUCION DE LA PROBLEMÁTICA?** Se debe analizar claramente lo que necesita la organización y seleccionar la mejor metodologia en cuanto al analisis y gestion de riesgos.

Fuente: Autores del proyecto

Adaptación: Comprende el ajuste de los sistemas naturales o humanos a los estímulos climáticos actuales o esperados o a sus efectos, con el fin de moderar perjuicios o explotar oportunidades beneficiosas.

Alerta: Estado que se declara con anterioridad a la manifestación de un evento peligroso.

Amenaza: Peligro latente de que un evento físico de origen natural, o causado, o inducido por la acción humana de manera accidental.

Análisis y evaluación del riesgo: Implica la consideración de las causas y fuentes del riesgo, sus consecuencias y la probabilidad de que dichas consecuencias puedan ocurrir.

Conocimiento del riesgo: Es el proceso de la gestión del riesgo compuesto por la identificación de escenarios de riesgo, el análisis y evaluación del riesgo, el monitoreo y seguimiento del riesgo y sus componentes.

Desastre: Es el resultado que se desencadena de la manifestación de uno o varios eventos naturales.

Emergencia: Situación caracterizada por la alteración o interrupción intensa y grave de las condiciones normales de funcionamiento u operación de una comunidad.

Gestión del riesgo: Es el proceso social de planeación, ejecución, seguimiento y evaluación de políticas y acciones permanentes para el conocimiento del riesgo y promoción de una mayor conciencia del mismo, impedir o evitar que se genere, reducirlo o controlarlo cuando ya existe y para prepararse y manejar las situaciones de desastre, así como para la posterior recuperación, entiéndase: rehabilitación y reconstrucción. Estas acciones tienen el propósito explícito de contribuir a la seguridad, el bienestar y calidad de vida de las personas y al desarrollo sostenible.

Intervención: Corresponde al tratamiento del riesgo mediante la modificación intencional de las características de un fenómeno con el fin de reducir la amenaza que representa o de modificar las características intrínsecas de un elemento expuesto con el fin de reducir su vulnerabilidad.

Manejo de desastres: Es el proceso de la gestión del riesgo compuesto por la preparación para la respuesta a emergencias, la preparación para la recuperación pos-desastre, la ejecución de dicha respuesta y la ejecución de la respectiva recuperación, entiéndase: rehabilitación y recuperación.

Mitigación del riesgo: Medidas de intervención prescriptiva o correctiva dirigidas a reducir o disminuir los daños y pérdidas que se puedan presentar a través de reglamentos de seguridad y proyectos de inversión pública o privada cuyo objetivo es reducir las condiciones de amenaza, cuando sea posible, y la vulnerabilidad existente.

Prevención de riesgo: Medidas y acciones de intervención restrictiva o prospectiva dispuestas con anticipación con el fin de evitar que se genere riesgo.

Reducción del riesgo: Es el proceso de la gestión del riesgo, está compuesto por la intervención dirigida a modificar o disminuir las condiciones de riesgo existentes, entiéndase: mitigación del riesgo y a evitar nuevo riesgo en el territorio, entiéndase: prevención del riesgo.

Riesgo de desastres: Corresponde a los daños o pérdidas potenciales que pueden presentarse debido a los eventos físicos peligrosos de origen natural, socio-natural tecnológico.

Vulnerabilidad[7]: Susceptibilidad o fragilidad física, económica, social, ambiental o institucional que tiene una comunidad de ser afectada o de sufrir efectos adversos en caso de que un evento físico peligroso se presente.

Análisis del riesgo: El uso sistemático de información disponible para determinar con qué frecuencia un determinado evento puede ocurrir y la magnitud de sus consecuencias.

Control. Medida que modifica el riesgo.

- Preventivos: aquellos que actúan para eliminar las causas del riesgo para
- prevenir su ocurrencia o materialización.
- Correctivos: Aquellos que permiten el restablecimiento de actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia

Mejora continua. Acción permanente realizada, con el fin de aumentar la capacidad para cumplir los requisitos y optimizar el desempeño.[8]

2.3 MARCO TEÓRICO

Un riesgo de un proyecto es un evento o condición incierto que, si se produce, tendrá un efecto positivo o negativo sobre al menos un objetivo del proyecto, como tiempo, coste, alcance o calidad, es decir, cuando el objetivo de tiempo de un proyecto es cumplir con el cronograma acordado; cuando el objetivo de coste del proyecto es cumplir con el coste acordado, etc.

[7] UNIDAD NACIONAL DE GESTIÓN DE RIESGOS DE DESASTRES. Glosario de términos de la gestión de riesgos de desastres. [En línea]. Publicado en internet en el año 2015. Ubicado en la URL: http://portal.gestiondelriesgo.gov.co/Paginas/Glosario_Terminos_Gestion_del_Riesgo.aspx

[8]MINISTERIO DEL INTERIOR Y JUSTICIA. Mejora continua. [En línea]. Ubicado en el URL: https://www.mininterior.gov.co/sites/default/files/guia_2.pdf

Las organizaciones perciben los riesgos por su relación con las amenazas al éxito del proyecto o por las oportunidades de mejorar las posibilidades de éxito del proyecto. Los riesgos que son amenazas para el proyecto pueden ser aceptados si el riesgo está en equilibrio con el beneficio que puede obtenerse al tomarlo.

Los riesgos que constituyen oportunidades, como la aceleración del trabajo que puede lograrse asignando personal adicional, pueden ser monitorizados para beneficiar los objetivos del proyecto.

El riesgo está compuesto de tres componentes esenciales:

- Un evento definible
- Probabilidad de ocurrencia
- Consecuencia de la ocurrencia (impacto)[9]

Otras de las características que distinguen a los riesgos son:

Los riesgos son situacionales: los riesgos varían drásticamente de una situación a otra. Un uso eficiente de las herramientas y técnicas puede ayudar a mitigar dichos riesgos.

Los riesgos pueden ser interdependientes: los riesgos a menudo están relacionados. La respuesta a un riesgo puede provocar un nuevo riesgo o aumentar el impacto de uno ya existente.

Los riesgos dependen de la magnitud: un determinado riesgo podría ser aceptado por ejemplo, si los beneficios y oportunidades potenciales son mayores.

Los riesgos están basados en valor: el nivel de tolerancia del riesgo varía de una persona a otra. Tanto las personas como la compañía influyen en la tolerancia al riesgo.

Los riesgos están basados en tiempo: el riesgo es un fenómeno del futuro causado por acciones actuales. El tiempo además afecta a la percepción del riesgo. Dependiendo de cuándo ocurra el riesgo, la percepción cambia.

Clasificación de riesgos. Usar categorías de riesgos ayuda a identificar nuevos riesgos. Las categorías pueden ser distintas dependiendo del tipo de proyecto. A continuación se proponen algunas:

Los riesgos se pueden clasificar según sus fuentes, es decir, según las causas que los provocan. Existen dos grandes categorías en la que agrupar las fuentes de los riesgos:

[9] ARCE SANTOLAYA. Rubén. El diario de empresarios y directivos. [En línea]. Publicado en internet el 20 de marzo de 2015. Ubicado en la URL: http://diarioempresariosydirectivos.blogspot.com.co/2015/03/gestion-del-riesgo-en-los-proyectos.html

- Fuentes de riesgos internos
- Fuentes de riesgos externos.

Los riesgos externos son aquellos que tienen sus fuentes fuera de la organización que esponsoriza el proyecto. Sin embargo, los riesgos internos tienen sus fuentes dentro de la organización, incluyendo el proyecto. Los riesgos internos pueden ser controlados por el equipo de proyecto.[10]

De igual forma se tomaron de base para el estudio de la propuesta las siguientes normas:

ISO 27001.[11] Sistema de Gestión de la Seguridad de la Información La norma/estándar UNE ISO/IEC 27001: 2007 del "Sistema de Gestión de la Seguridad de la Información" es la solución de mejora continua más adecuada para evaluar los riesgos físicos (incendios, inundaciones, sabotajes, vandalismos, accesos indebidos e indeseados) y lógicos (virus informáticos, ataques de intrusión o denegación de servicios) y establecer las estrategias y controles adecuados que aseguren una permanente protección y salvaguarda de la información.

ISO/IEC 27002.[12] La información es crítica para la operación y, en casos extremos, para la supervivencia de las organizaciones. Usando un Sistema de Gestión de Seguridad de la Información (SGSI) y certificándolo contra el estándar ISO/IEC 27001, ayudará a las organizaciones a gestionar y proteger sus activos de información.

La ISO/IEC 27001:05[13]. nace como modelo para gestionar la seguridad de la información y, como todos los modelos ISO certificables, no se refiere a un contexto específico, es decir, que el modelo también es aplicable fuera de los sistemas informáticos, siendo la información entendida como independiente de los soportes y de las infraestructuras.

En general se puede afirmar que el modelo es aplicable a cualquier contexto productivo y a cualquier tipo de organización: simple o compleja, pública o privada, informatizada o no. La experiencia nos enseña, sin embargo, que quienes lo emplean con mayor frecuencia y eficacia son las empresas y las organizaciones para las que las TICs constituye un eje portante de relieve (administraciones públicas centrales y locales, proveedores de servicios telefónicos y de telecomunicaciones, departamentos/divisiones IT de bancos y seguros, etc.).

---

[10] PMBOOK GESTION. Riesgos. [En línea]. Ubicado en la URL: http://pmbok1.blogspot.com/p/blog-page_2251.html

[11] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI). Bogotá D.C.: ICONTENC, 2006. NTC ISO/IEC 27001.

[12] 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.

[13] Ibíd. NTC 27002.

NTC 5254[14] .Norma técnica Colombiana para le gestión de riesgos adoptada de la norma AS/NZ 4360:2004 es una guía genérica que sirve como fuente de verificación de definiciones y procesos de documentación.

ISO/IEC 27005[15]**.** Guía para la gestión del riesgo en relación a la seguridad de la información.

2.4 MARCO LEGAL

La propuesta de investigación sobre la guía de gestión de riesgos de tecnologías de la información para el proceso de Consulta Externa de la IPS Dr Prosalud S.A.S estará sujeta a la siguiente legislación:

Ley 527 de 1999 por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Ley 23 de 1982 por la cual se decreta las disposiciones generales sobre derechos de autor.

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

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

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

[14] NTC 5254. Fundamentos de la gestión de riesgo. [En línea]. Ubicado en la URL: http://www.pascualbravo.edu.co/pdf/calidad/gestionriesgos.pdf

[15] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información. Bogotá D.C.: ICONTEC, 2009. NTC ISO/IEC 27005.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

El proyecto está definido mediante un tipo de investigación descriptiva con el fin de determinar situaciones y características de la IPS Dr. Prosalud S.A.S

3.2 POBLACIÓN Y MUESTRA

La población está conformada por el personal que labora en Consulta Externa de la IPS Dr Prosalud S.A.S. De igual manera, como en esta área el personal no supera las 10 personas se tomara como muestra el 100% de la población que está involucrada en este proceso

3.3 TECNICAS E INTRUMENTOS

Para el desarrollo de este proyecto de investigación se implementarán las técnicas y herramientas de desarrollo metodológico como:

- Observación directa mediante visitas en la IPS Dr Prosalud S.A.S. y listas de chequeo para verificar validez y confiabilidad de la información con el fin de obtener buenos resultados.

- Revisión documental de los procesos que la IPS Dr. Prosalud S.A.S. con el fin de tener soporte y permitir hacer una idea del desarrollo y las características de los procesos

- Entrevistas y encuestas a los implicados en el proceso de consulta externa de la IPS. con el fin de analizar el proceso y diseñar la información que no está soportada.

Cuadro 3. Objetivos y actividades

Objetivo específico	Actividades	Entregable
Diseñar el Modelo del Negocio del proceso de Consulta Externa de la IPS Dr Prosalud S.A.S.	Realizar visita a la IPS Dr Prosalud para identificar los procesos de la empresa	Modelo del Negocio
	Identificar el Mapa de Procesos	
	Identificar los procesos y subprocesos de apoyo.	
	Identificar la infraestructura tecnológica de la IPS Dr. Prosalud S.A.	
Diagnosticar el estado actual del proceso de Consulta	Elaborar instrumentos de recolección de información	Informe auditoria pasiva basada en NTC-ISO-IEC-

Externa de la IPS Dr Prosalud S.A.S. por medio de una auditoria pasiva basada en NTC-ISO-IEC-27001	Aplicar los instrumentos de recolección de la información en la IPS Dr. Prosalud S.A.	27001
	Análisis de los resultados obtenidos en la aplicación de instrumentos de recolección de información	Dictamen de la auditoria
	Realizar búsqueda documental para dar soporte a la auditoria	
Crear una guía de gestión de riesgos como apoyo a la seguridad de la información para el proceso de Consulta Externa de la IPS Dr Prosalud S.A.S..	Realizar un análisis de las metodologías de gestión de riesgos actuales.	Guía de Gestión de Riesgos para el proceso de Consulta Externa de la IPS Dr Prosalud S.A.S.
	Seleccionar la metodología de gestión de riesgos que se adapta al proceso de la IPS Dr Prosalud S.A.S.	
	Realizar una guía de Gestión de riesgos para el proceso de Consulta Externa de la IPS Dr Prosalud S.A.S.	

Fuente: Autores del proyecto

4. PRESENTACION DE RESULTADOS

4.1 MODELO DEL NEGOCIO DEL PROCESO DE CONSULTA EXTERNA DE LA IPS DR PROSALUD S.A.S.

4.1.1 Misión y Visión de la IPS Dr. Prosalud S.A.S.

Misión

Somos una IPS con mayor proyección y cobertura para la población en general, comprometidos con el bienestar de las familias mediante la prestación de servicios de alta calidad, generando relaciones trascendentales y perdurables. Nuestra experiencia nos permite un rápido y fácil afrontamiento de las necesidades de la población con conciencia y animo social.

Visión

Ser una empresa con equidad, que en los años venideros logremos el liderazgo que nos permita crecer bajo los pilares de la honestidad, respeto y solidaridad, causando un mayor impacto en la población, ofreciendo y manteniendo servicios con excelencia.

4.1.2 Objetivos Organizacionales de la IPS Dr. Prosalud S.A.S.

En desarrollo de la misión de DR PROSALUD IPS S.A.S tendrá los siguientes objetivos corporativos que constituirán el accionar empresarial:

✓ Consolidar el sistema obligatorio de Garantía de calidad con miras a alcanzar la acreditación.

✓ Mantener la viabilidad financiera y sostenibilidad económica de la entidad.

✓ Consolidar a la IPS como empresa líder en la prestación de los servicios de salud.

✓ Fortalecimiento de la infraestructura y los procesos para la prestación de servicios con calidad humanizada.

4.1.3 Principios y Valores Corporativos de la IPS Dr Prosalud S.A.S.

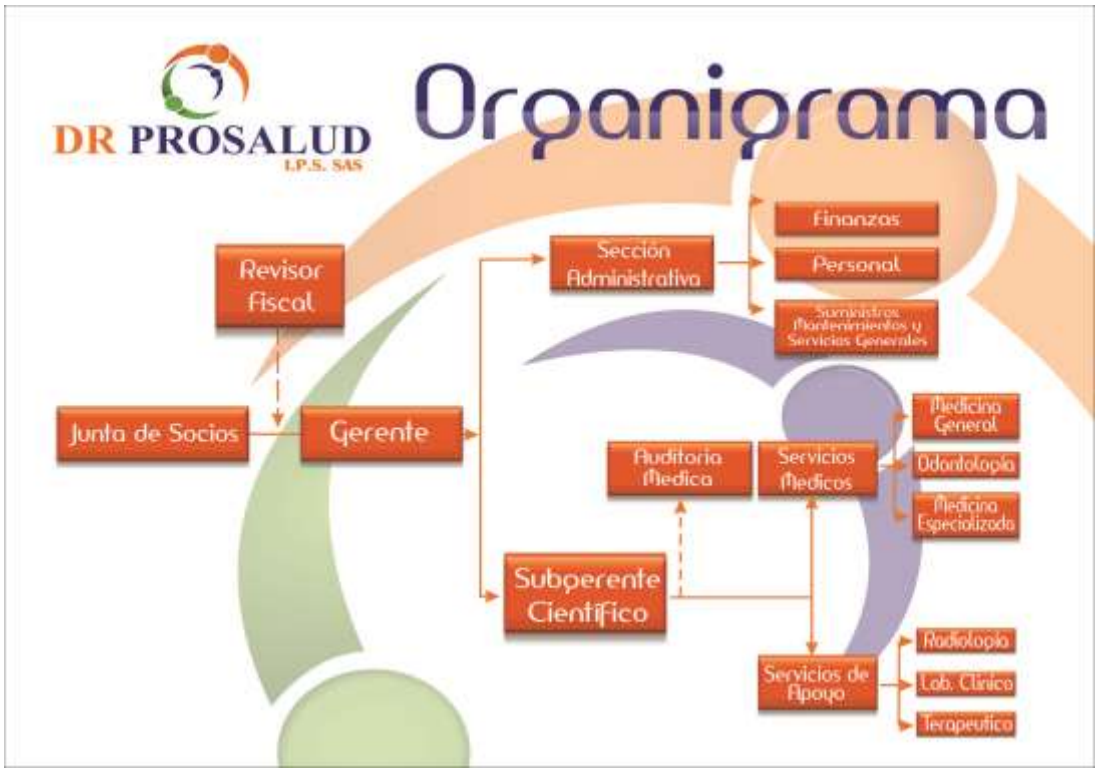
En la figura 1 se ilustra los valores corporativos que tiene la IPS Dr. Prosalud S.A.S. y por ende son los pilares que diariamente definen el desarrollo y ambiente corporativo. Se deben mantener constantemente estos principios para mantener las buenas relaciones personales tanto con el personal administrativo como con los visitantes.

Figura 2. Valores Corporativos de la IPS Dr Prosalud S.A.S.

Fuente: DR PROSALUD

4.1.4 Estructura Orgánica de la IPS Dr Prosalud S.A.S. La IPS Dr. Prosalud S.A.S. es una institución prestadora de servicios de salud que ofrece servicios humanizados con Calidad y Responsabilidad Social. Su organización es como esta descrita en la Figura 2. en forma horizontal describiendo la jerarquía y áreas que lo integran para poder manejar la información como un todo y tenga una mejor fluidez.

Figura 3. Organigrama de la IPS Dr. Prosalud S.A.S.



Fuente: DR PROSALUD

4.1.5. Mapa de Procesos de la IPS Dr Prosalud S.A.S.

La IPS Dr. Prosalud S.A.S. maneja el mapa de procesos que se puede apreciar en la Figura 3. donde se ofrece una visión general de un sistema de gestión, están representados uno a uno los procesos de dirección, procesos misionales y procesos de apoyo. Cada uno de estos procesos viene relacionados entre si indicando como fluye la información.

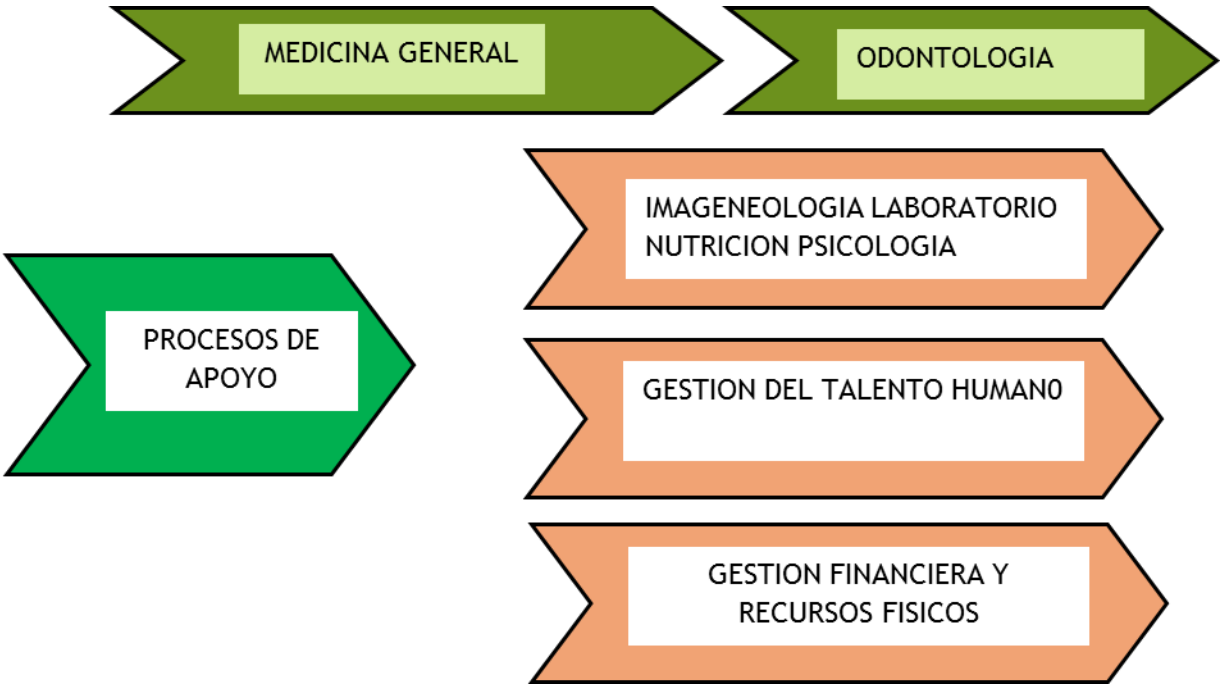
Figura 4. Mapa de Procesos de la IPS Dr. Prosalud S.A.S.

Fuente: DR PROSALUD

4.1.6 Cadena de Valor de la dependencia Consulta Externa

El proceso a analizar en el estudio de Auditoria de Sistemas según el organigrama es: Servicios Médicos (Consulta Externa). Teniendo en cuenta que Medicina General y Medicina Especializada se tomó como un solo proceso.

Figura 5. Cadena de de la IPS Dr. Prosalud S.A.S.



Fuente: Autores del proyecto

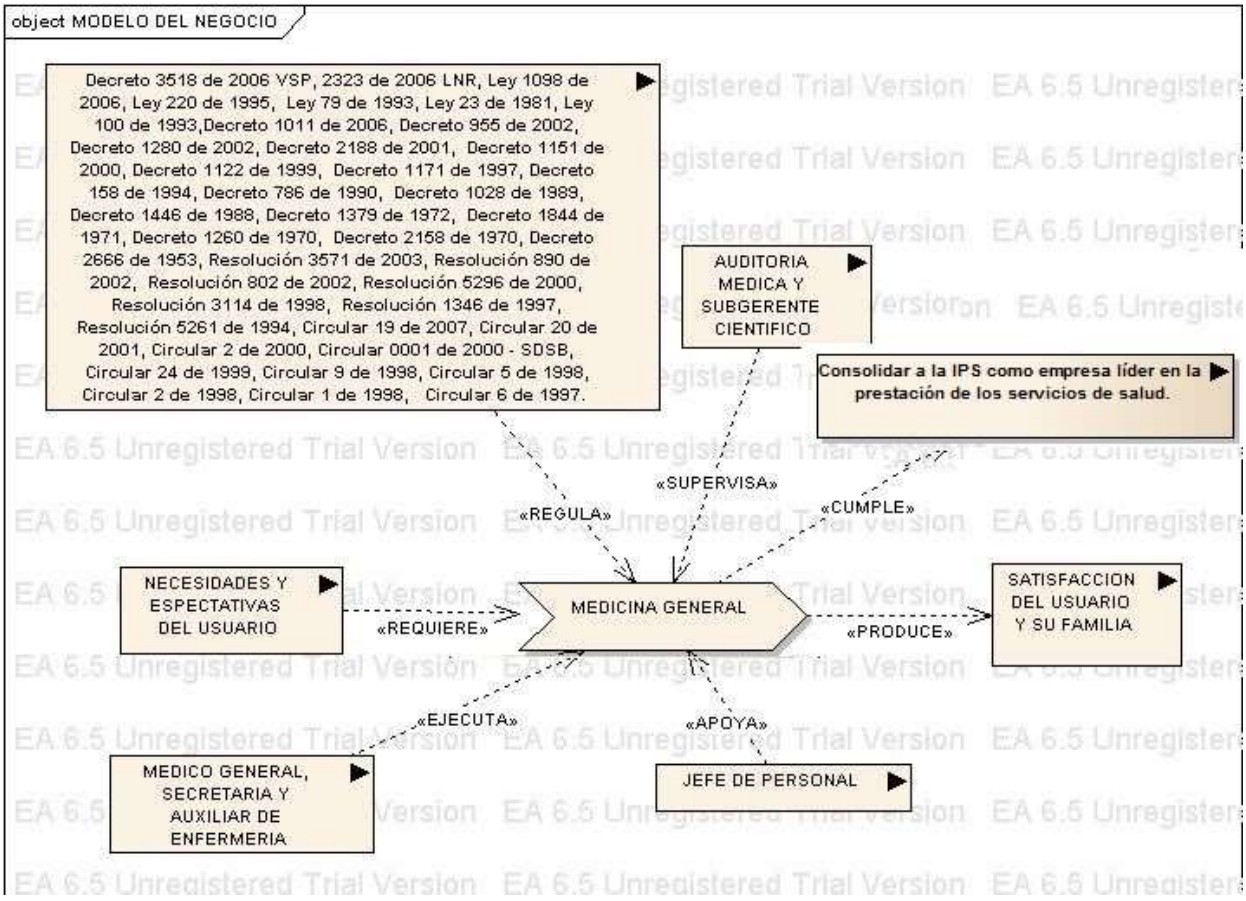
4.1.7 Procesos y Subprocesos de la dependencia Consulta Externa

Para el desarrollo de este análisis se tuvo en cuenta el mapa de procesos de la IPS Dr. Prosalud S.A.S. enfocado en el Organigrama.

Proceso Medicina General de la dependencia de Consulta Externa de la IPS Dr. Prosalud S.A.S.

En éste proceso se deben diagnosticar y resolver con tratamiento médico y con procedimientos sencillos la mayoría de los padecimientos que el ser humano sufre en su vida, desde niño hasta la vejez, con acciones frecuentemente realizadas en el consultorio del médico o en la casa del enfermo, dicho proceso es realizado por una persona con el conocimiento y destrezas necesarias como lo es el médico general.

Figura 6. Proceso Medicina General de la IPS DR Prosalud S.A.S

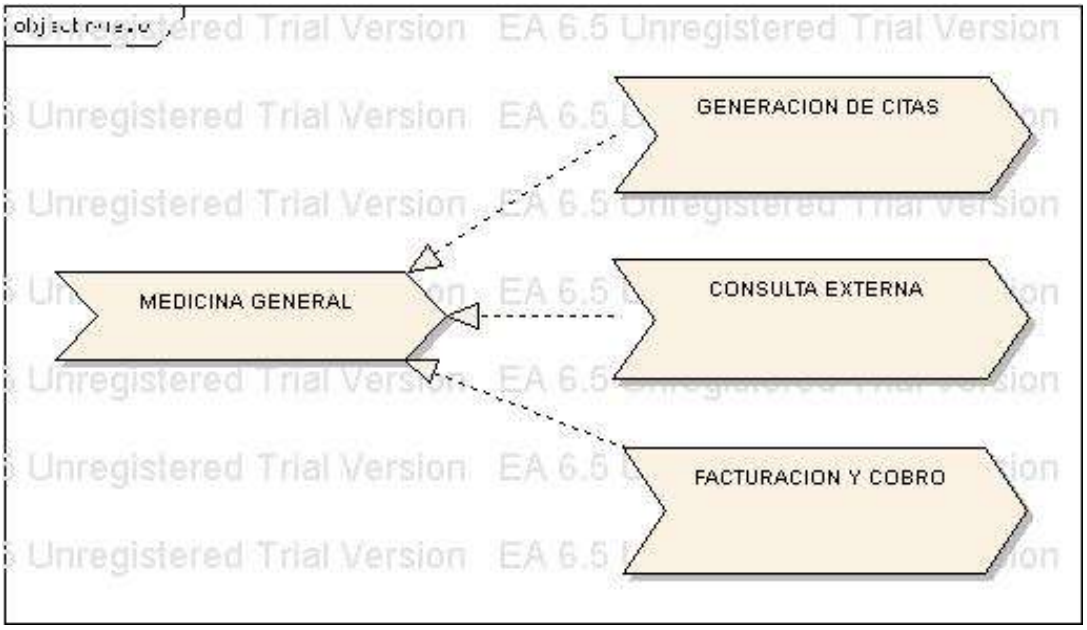


Fuente: Autores del proyecto

Subprocesos Medicina General de la IPS Dr. Prosalud S.A.S.

Del proceso de Medicina General se dividen tres subprocesos que son generación de citas, consulta externa y facturación y cobro los cuales se ven a continuación.

Figura 7. Subprocesos Medicina General de la IPS DR Prosalud S.A.S

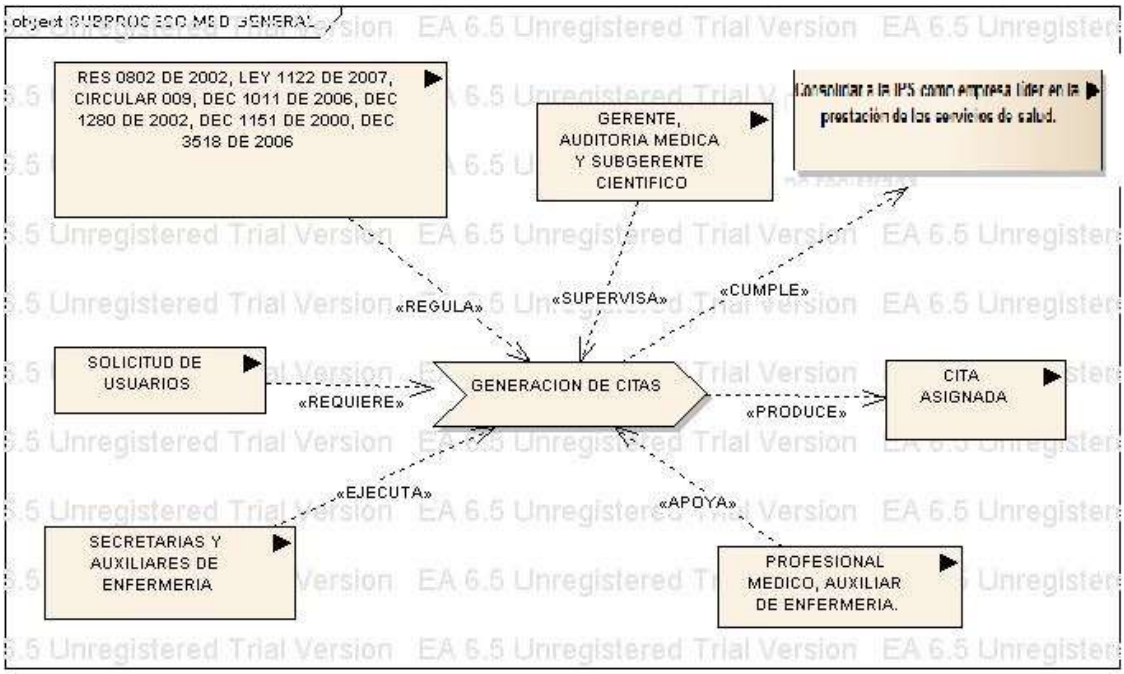


Fuente: Autores del proyecto

Subproceso de Generación de Citas de la IPS DR Prosalud S.A.S

El subproceso generación de citas está relacionado a la asignación de la agenda de los médicos con el fin de mantener un orden que debe cumplirse todo los días, dicha solicitud la realizan los usuarios de la clínica y es ejecutada por la secretaria y/o auxiliares de enfermería.

Figura 8. Subprocesos de Generación de Citas de la IPS DR Prosalud S.A.S

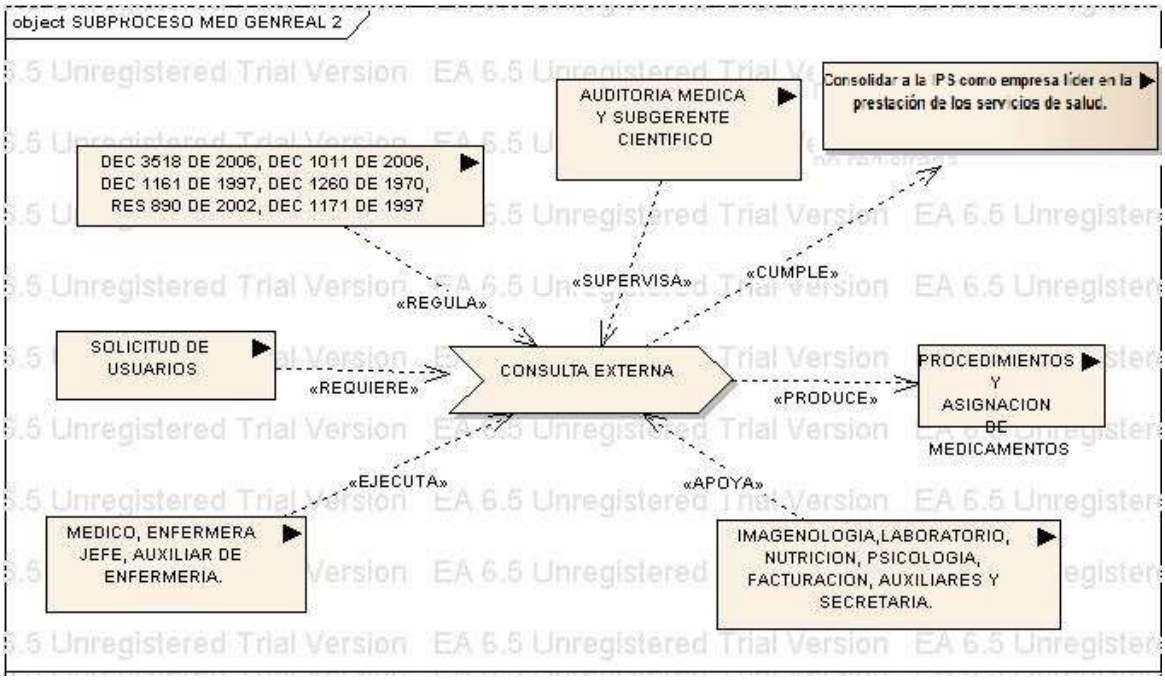


Fuente: Autores del proyecto

Consulta Externa de la IPS DR Prosalud S.A.S

La revisión y diagnóstico médico de los pacientes de la IPS Dr Prosalud S.A.S da lugar a los procesos que a ellos se le asignan, así como los exámenes de laboratorio y otros que sean necesario para una completa revisión y así poder asignar el mejor tratamiento.

Figura 9. Subprocesos de Consulta Externa de la IPS DR Prosalud S.A.S

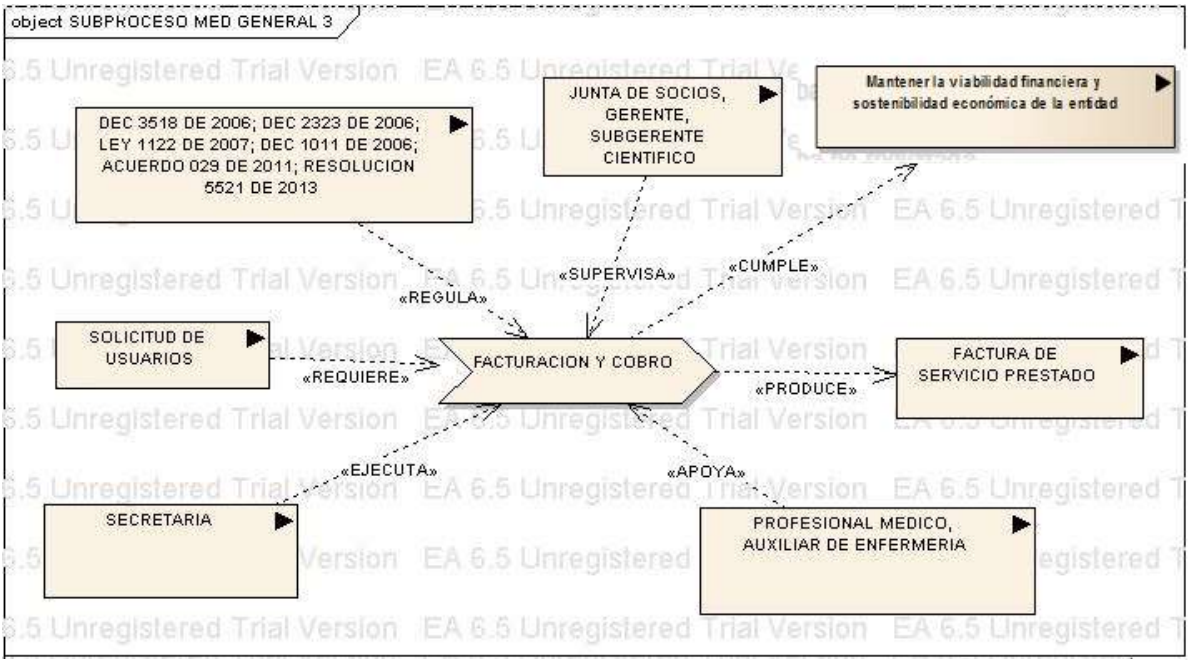


Fuente: Autores del proyecto

Facturación y Cobro de la IPS DR Prosalud S.A.S

Proceso en el cual después de ser valorado los pacientes por los médicos de la clínica y haber recetado los medicamentos y/o procedimientos necesarios para éste, son generadas las cuentas de cobro correspondientes a los tratamientos realizados a cada paciente.

Figura 10. Subprocesos de Facturación y Cobro de la IPS DR Prosalud S.A.S

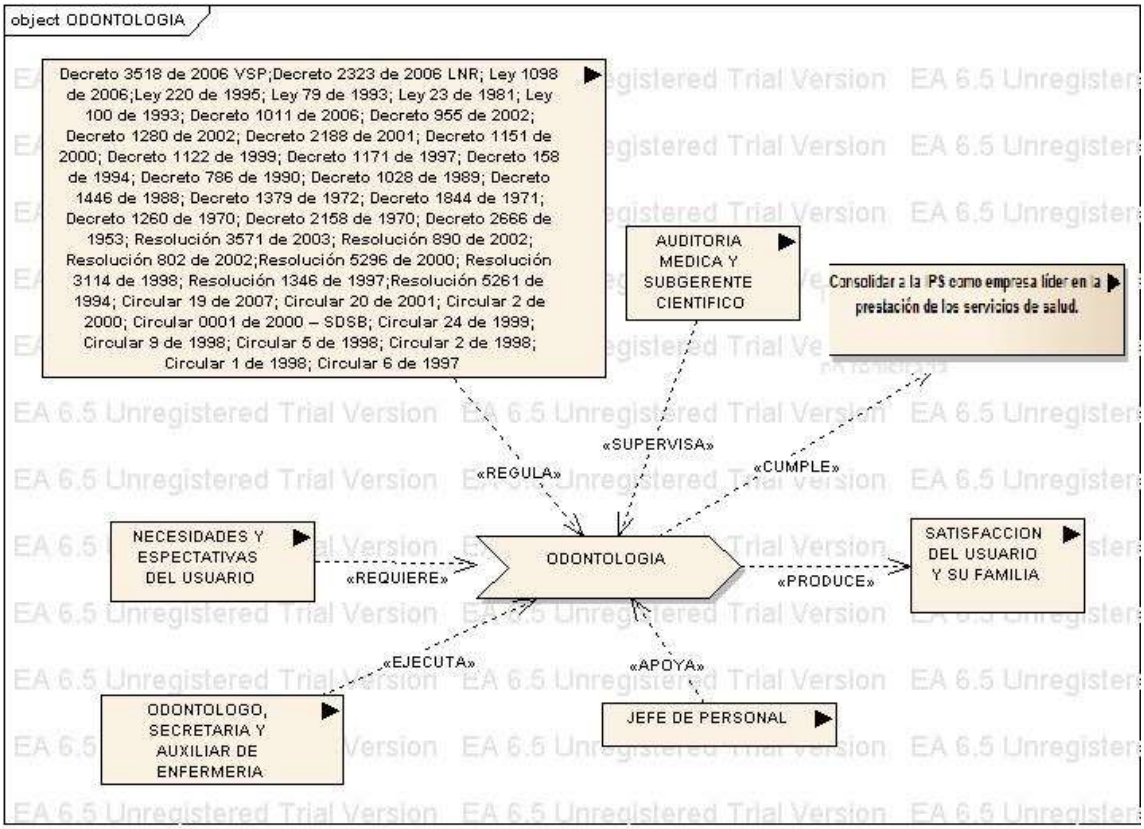


Fuente: Autores del proyecto

Proceso Odontología de la dependencia de Consulta Externa Externa de la IPS Dr. Prosalud S.A.S.

En éste proceso se deben diagnosticar y resolver con tratamiento médico y con procedimientos sencillos la mayoría de los padecimientos que el ser humano sufre en su vida, desde niño hasta la vejez, con acciones frecuentemente realizadas en el consultorio odontologico, dicho proceso es realizado por una persona con el conocimiento y destrezas necesarias como lo es el médico general.

Figura 11. Proceso Odontología de la IPS DR Prosalud S.A.S

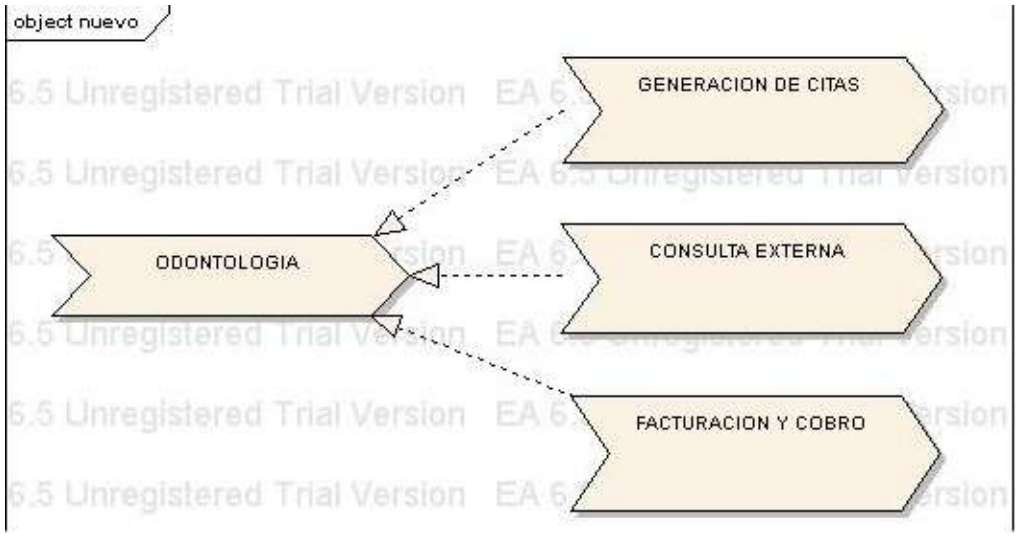


Fuente: Autores del proyecto

Subproceso Odontología de la IPS Dr. Prosalud S.A.S.

El servicio odontológico se presta para brindar salud oral o bucal a todos los usuarios que soliciten servicio en la clínica IPS Dr. Prosalud S.A.S. dentro de éste se encuentran los subprocesos de generación de citas, consulta odontológica y facturación y cobro.

Figura 12. Subproceso Odontología de la IPS DR Prosalud S.A.S

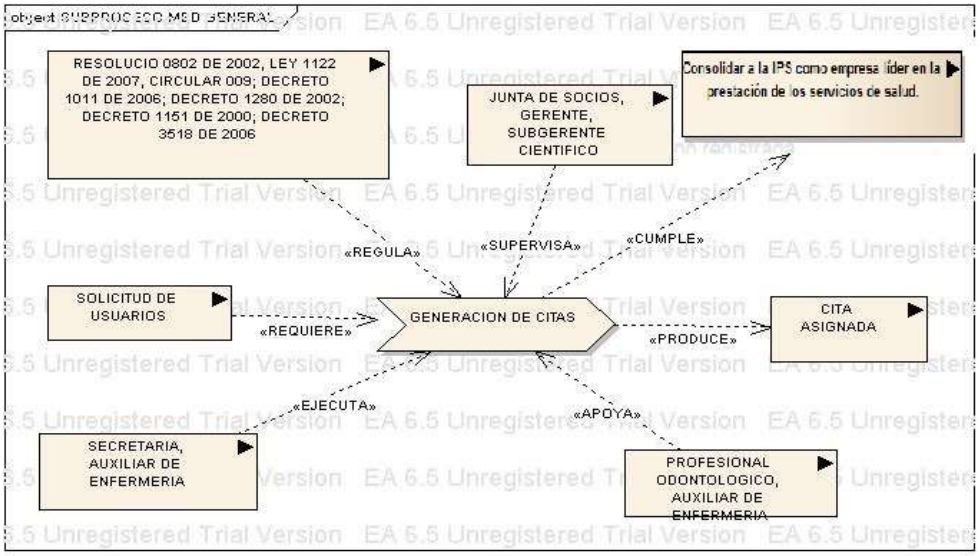


Fuente: Autores del proyecto

Subprocesos de Generación de Citas de la IPS DR Prosalud S.A.S

El subproceso generación de citas está relacionado a la asignación de la agenda de los odontólogos con el fin de mantener un orden que debe cumplirse todo los días, dicha solicitud la realizan los usuarios de la clínica y es ejecutada por la secretaria y/o auxiliares de enfermería.

Figura 13. Subprocesos de Generación de Citas de la IPS DR Prosalud S.A.S

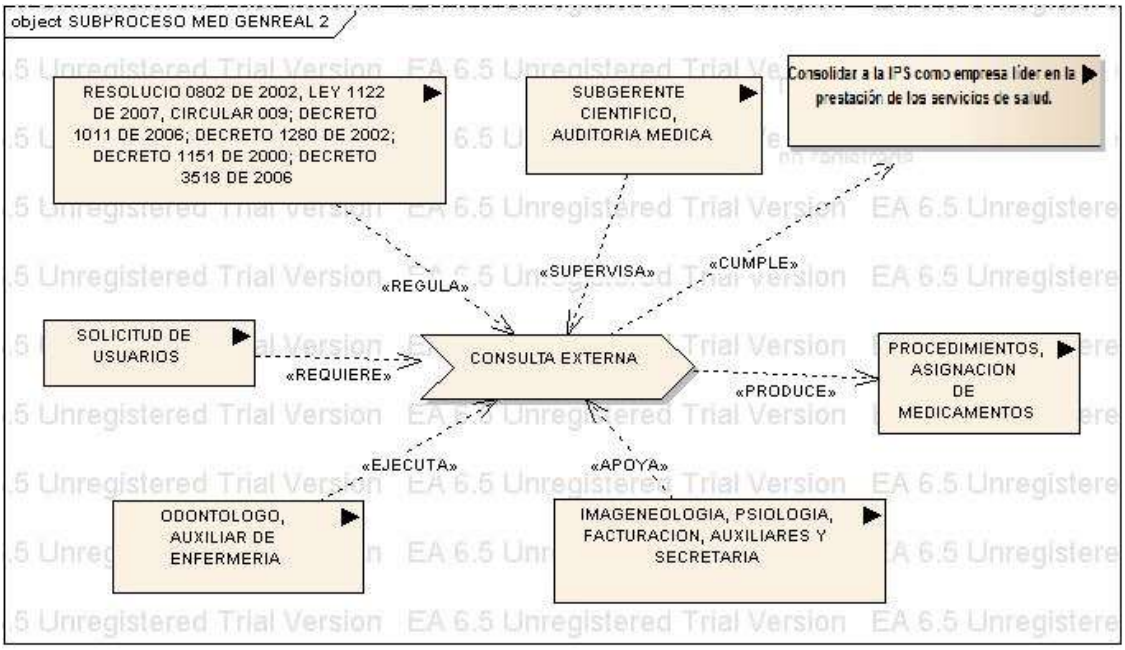


Fuente: Autores del proyecto

Subprocesos de Consulta Externa de la IPS DR Prosalud S.A.S

La revisión y diagnóstico odontológico de los pacientes de la IPS Dr Prosalud S.A.S da lugar a los procesos que a ellos se le asignan, así como los exámenes de rayos x y otros que sean necesario para una completa revisión y así poder asignar el mejor tratamiento.

Figura 14.Subprocesos de Consulta Externa de la IPS DR Prosalud S.A.S

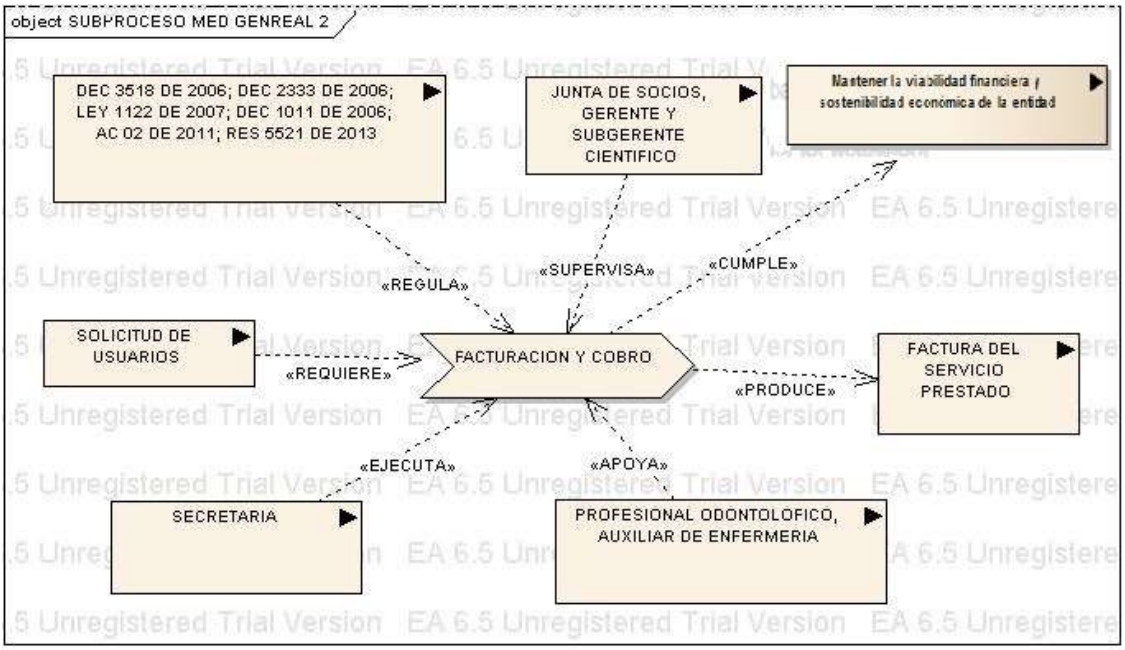


Fuente: Autores del proyecto

Subprocesos de Facturacion y Cobro de la IPS DR Prosalud S.A.S

Proceso en el cual después de ser valorado los pacientes por los odontólogos de la clínica y haber recetado los medicamentos y/o procedimientos necesarios para éste, son generadas las cuentas de cobro correspondientes a los tratamientos realizados a cada paciente.

Figura 15. Subprocesos de Facturacion y Cobro de la IPS DR Prosalud S.A.S



Fuente: Autores del proyecto

4.1.8 Modelo de Actores de la IPS DR. Prosalud S.A.S.

El modelo de Actores de la IPS DR. Prosalud S.A.S. describe de qué manera intervienen los dos procesos principales como lo son medicina general y odontología y las responsabilidades para el mejor desempeño del mismo. De ogial manera la IPS Dr. Prosalud S.A.S. no tenía documentado un modelo de actores por lo cual se definió el siguiente por el grupo auditor.

Proceso medicina general de la IPS DR. Prosalud S.A.S.

En el proceso de medicina general de la IPS DR. Prosalud S.A.S. nos muestra la viabilidad en el desarrollo de actividades dentro de la organización es por esto que están organizados en subprocesos para llevar el control adecuado en la supervisión, ejecución y apoyo y de cada uno de los actores que intervienen en cada subproceso.

PROCESO MEDICINA GENERAL			
SUBPROCESO GENERACIÓN DE CITAS			
ACTOR	**EJECUTA**	**SUPERVISA**	**APOYA**
Gerente		**X**	
Subgerente Científico		**X**	
Auditoria Medica		**X**	
Profesional (Medico)			**X**
Auxiliar de Enfermería			**X**
Secretaria	**X**		

Fuente: Autores del Proyecto

SUBPROCESO CONSULTA EXTERNA			
ACTOR	**EJECUTA**	**SUPERVISA**	**APOYA**
Gerente		**X**	
Subgerente Científico			**X**
Auditoria Medica		**X**	
Profesional (Medico)	**X**		
Auxiliar de Enfermería			**X**
Secretaria			**X**

Fuente: Autores del Proyecto

SUBPROCESO FACTURACION Y COBRO			
ACTOR	**EJECUTA**	**SUPERVISA**	**APOYA**
Gerente	**X**		
Subgerente Científico		**X**	
Auditoria Medica		**X**	
Profesional (Medico)			**X**
Auxiliar de Enfermería			**X**
Secretaria	**X**		

Fuente: Autores del Proyecto

Proceso de Odontología de la IPS DR. Prosalud S.A.S.

En el proceso de odontologia de la IPS DR. Prosalud S.A.S. nos muestra la viabilidad en el desarrollo de actividades dentro de la organización es por esto que están organizados en subprocesos para llevar el control adecuado en la supervisión, ejecución y apoyo y de cada uno de los actores que intervienen en cada subproceso.

PROCESO ODONTOLOGIA			
SUBPROCESO GENERACIÓN DE CITAS			
ACTOR	**EJECUTA**	**SUPERVISA**	**APOYA**
Gerente		**X**	
Subgerente Científico		**X**	
Auditoria Medica		**X**	
Profesional (Odontólogo)			**X**
Auxiliar de Enfermería			**X**
Secretaria	**X**		

Fuente: Autores del Proyecto

SUBPROCESO CONSULTA EXTERNA			
ACTOR	**EJECUTA**	**SUPERVISA**	**APOYA**
Gerente		**X**	
Subgerente Científico			**X**
Auditoria Medica		**X**	
Profesional (Odontólogo)	**X**		
Auxiliar de Enfermería			**X**
Secretaria			**X**

Fuente: Autores del Proyecto

SUBPROCESO FACTURACION Y COBRO			
ACTOR	**EJECUTA**	**SUPERVISA**	**APOYA**
Gerente	**X**		
Subgerente Científico		**X**	
Auditoria Medica		**X**	
Profesional (Odontologo)			**X**
Auxiliar de Enfermería			**X**
Secretaria	**X**		

Fuente: Autores del Proyecto

4.1.9 Infraestructura tecnología

Personal a Cargo de las T.I.

Se realiza el análisis a la estructura orgánica de DR PROSALUD IPS S.A.S. con el fin de determinar el personal a cargo de las T.I.

Se definieron de la siguiente manera:

- ✓ Director Ejecutivo (CEO): Junta de Socios

- ✓ Director Financiero (CFO); Junta de Socios
- ✓ Ejecutivo del Negocio: Junta de Socios

- ✓ Director de Información (CIO): Subgerente Científico

- ✓ Propietario del proceso del negocio: Gerente

- ✓ Jefe de Operaciones: Gerente

- ✓ Jefe de Desarrollo: Asesor Externo en TI

- ✓ Arquitecto en Jefe: Asesor Externo en TI

- ✓ Jefe de Administración de TI: Gerente

- ✓ La oficina de administración de proyectos (PMO): Subgerente Científico

- ✓ Cumplimiento, auditoría, riesgo y seguridad.: Auditoria Medica

Tipo de Red

En la empresa DR Prosalud IPS S.A.S. presenta un tipo de red LAN (Local Área Network, redes de área local) inalámbrica dentro de sus instalaciones como medio de comunicación para el desarrollo de sus procesos manteniendo una distribución lógica cliente-servidor. Así mismo maneja un tipo de red WAN (Wide Area Network, redes de área extensa) con el outsourcing (Asesor Técnico TI) como forma de apoyo y respaldo de la información.

Topología de Red

La topología que utiliza DR Prosalud IPS S.A.S. es una red en estrella en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de éste. Los dispositivos no están directamente conectados entre sí, además de que no se permite tanto tráfico de información. Dada su transmisión, una red en estrella activa tiene un nodo central (router) activo que normalmente tiene los medios para prevenir problemas relacionados con el eco. Lo que facilita posee que pueda agregar nuevos equipos fácilmente, reconfiguración rápida, fácil de prevenir daños y/o conflictos, centralización de la red, es simple de conectar

Recursos Tecnológicos

En la dependencia a analizar posee tres computadores para el desarrollo de la actividad en cada consultorio y un servidor ubicado en la recepción.

Se describen a continuación las características básicas:

Consultorio 1:	
Pc de Escritorio	Procesador Intel Celeron Duo 2.40Ghz Memoria Ram 2Gb Sistema Operativo: Windows 7 32 btis
Consultorio 2:	
Pc de Escritorio	Procesador Intel Celeron CPU G1840 Memoria Ram 2Gb Sistema Operativo: Windows 8 Pro 64btis
Consultorio 3	
Pc de Escritorio	Procesador Intel Celeron CPU G1610 Memoria Ram 2Gb Sistema Operativo: Windows 8 Pro 64 btis
Servidor: **Consultorio 1:**	
Pc de Escritorio	Procesador Intel Celeron Duo 2.40Ghz Memoria Ram 2Gb Sistema Operativo: Windows 7 de 32 btis

Fuente: Autores del Proyecto

Además cada uno de estos equipos posee el siguiente software que le permite servir de apoyo en sus funciones:

- ✓ Xenia, Historia Clínica Especializada
- ✓ Microsoft Office 2010
- ✓ Antivirus AVG

4.2 ESTADO ACTUAL DEL PROCESO DE CONSULTA EXTERNA DE LA IPS DR PROSALUD S.A.S. POR MEDIO DE UNA AUDITORIA PASIVA BASADA EN NTC-ISO-IEC-27001

Durante el desarrollo de este proceso se tuvieron en cuenta los instrumentos de recolección de información documentados en el Anexo.

4.2.1 Presentación del grupo auditor

Para poder empezar a realizar formalmente el desarrollo de la auditoria se envio a la junta de socios el siguiente oficio con el fin de poder tener acceso a la información que se iba a evaluar

Ocaña, 1 de Junio de 2015

Doctor
DORIAN ENRIQUE RIVERA
Gerente General
DR PROSALUD IPS S.A.S
E.S.D

Me permito remitir a Usted el informe de resultados de la auditoría realizada a las instalaciones de la dependencia del Área de Consulta Externa de la IPS DR PROSALUD, con fecha inicial de 27 de Abril de 2015 y fecha de finalización 31 de Mayo de 2015.

Equipo Auditor

4.2.2 Programa de auditoria

En el siguiente programa de auditoria se describe las fases en las cuales se dividió el proceso de evaluación y las actividades a realizar para desarrollar la labor con su respectivo periodo de tiempo

OBJETIVO DE LA AUDITORIA. Evaluar la eficacia de los procesos del Sistema de información en el área de consulta externa de la IPS Dr Prosalud S.A.S. y establecer al mismo tiempo alternativas de solución

ALCANCE DE LA AUDITORIA. El desarrollo de la auditoria se basará en el análisis del proceso de Historia Clínica del Sistema de Información Xenia, Historia Clínica Especializada en el área de Consulta externa verificando la seguridad de la información.

FASE	DESCRIPCIÓN	ACTIVIDAD	No. Pers	PERIODO		DIAS HAB.
				INICIO	FIN	
1. EVALUACION ADMINISTRATIVA	En esta fase se evaluará la estructura de la empresa junto con sus metas políticas y planes.	Estudio de la estructura organizacional de la empresa del Área de Consulta Externa	2	27/04/15	29/04/15	3
		Evaluación de las normas y políticas de la organización del Área de Consulta Externa	2	04/05/15	05/05/15	2
2. EVALUACIÓN DE SISTEMAS Y PROCEDIMIENTOS	En esta fase se evaluará el funcionamiento de los sistemas de información verificando la	Evaluación del sistema de información y sus procedimientos en el Área de Consulta Externa	3	06/05/15	08/05/15	3

	existencia de los diversos manuales que éstos deben tener para un mejor uso por parte de los usuarios.	Comprobación de la existencia y estructura del manual de usuario.	1	11/05/15	11/05/15	1
		Análisis del módulo Historia Clínica del sistema de información en el Área de Consulta Externa.	2	12/05/15	14/05/15	2
3. EVALUACIÓN DE LOS EQUIPOS	En esta fase se evaluarán los equipos de cómputo, su, capacidad y mantenimiento.	Evaluación de la adquisición de licencias de software adquiridos en el área de consulta externa.	1	14/05/15	14/05/15	1
		Verificación de acceso en la utilización de los equipos en el área de Consulta Externa.	2	15/05/15	15/05/15	1
		Evaluación de la capacidad de almacenamiento de información y demás especificaciones de los equipos.	2	18/05/15	18/05/15	1
4. EVALUACIÓN DE LA SEGURIDAD.	En esta fase se evaluará la seguridad de la información en	Análisis de la seguridad en cuanto a la realización de	2	19/05/15	19/05/15	1

	cuanto a las copias de seguridad y los métodos utilizados para proteger los equipos.	copias de seguridad del sistema de información.				
		Verificación de la existencia de seguros que se adquieren para cada uno de los equipos del Área de Consulta Externa	1	20/05/15	20/05/15	1
5. APLICACIÓN DE PRUEBAS	En esta fase se aplicaran las respectivas pruebas que confirmen el funcionamiento del sistema de información del área de Consulta Externa, recolectando la información precisa para realizar un determinado dictamen.	Aplicar las pruebas pertinente en el Sistema de Información del área de Consulta Externa	3	21/05/15	25/05/15	3
6. ELABORACION DEL INFORME (DICTAMEN)	En esta fase se elaborara el dictamen en donde se plasmaran los hallazgos encontrados del Sistema de Información con las recomendaciones respectivas para el	Organización y análisis de la información recopilada.	3	26/05/15	26/05/15	1
		Realización del dictamen.	3	27/05/15	29/05/15	3
		Entrega del dictamen.	3	01/06/15	01/06/15	1

	mejoramiento de los procesos en el área de Consulta Externa					

Fuente: Autores del proyecto

4.2.3 Guía de auditoria

En la siguiente guía de auditoria se realizó un análisis de cada una de las actividades a realizar para la evaluación del proceso de consulta externa en la IPS Dr. Prosalud S.A.S. y se determinó que técnicas de evaluación con el fin de validar la información.

OBJETIVO DE LA AUDITORIA. Evaluar la eficacia de los procesos del Sistema de información en el área de consulta externa de la IPS Dr Prosalud S.A.S.. y establecer al mismo tiempo alternativas de solución

ALCANCE DE LA AUDITORIA. El desarrollo de la auditoria se basará en el análisis del proceso de Historia Clínica del Sistema de Información Xenia, Historia Clínica Especializada en el área de Consulta externa verificando la seguridad de la información.

REF.	FECHA	ACTIVIDAD O FUNCION A EVALUAR	TECNICA DE EVALUACION	OBSERVACIONES
GA. 01	27/04/15	Estudio de la estructura organizacional de la empresa en el Área de Consulta Externa	-Solicitar la Información pertinente. -Realizar entrevista al Subgerente Científico.	
GA. 02	04/05/15	Evaluación de las normas y políticas de la organización en el Área de Consulta Externa	-Solicitar la Información pertinente. -Realizar entrevista al Subgerente Científico. -Aplicación de la encuesta al Personal Medico	

GA. 03	06/05/15	Evaluación del sistema de información y sus procedimientos en el Área de Consulta Externa	-Realización de pruebas al Módulo de Historia Clínica. -Aplicar lista de chequeo	
GA. 04	11/05/15	Comprobación de la existencia y estructura del manual de usuario.	-Solicitar la Información pertinente. -Aplicar lista de chequeo	
GA. 05	12/05/15	Análisis del módulo Historia Clínica del sistema de información en el Área de Consulta Externa.	-Realizar pruebas a modulo del sistema información. -Aplicar lista de chequeo	
GA. 06	14/05/15	Evaluación de la adquisición de licencias de software adquiridos en el área de consulta externa.	-Solicitar la Información pertinente. -Realizar entrevista al Subgerente Científico.	
GA. 07	15/05/15	Verificación de las políticas de acceso de los equipos en el área de Consulta Externa.	-Realizar pruebas a de acceso al sistema de información. -Aplicar lista de chequeo	
GA. 08	18/05/15	Evaluación de la capacidad de almacenamiento de información y demás especificaciones de los equipos.	-Solicitar la Información pertinente. -Aplicar lista de chequeo	
GA. 09	19/05/15	Análisis de la seguridad en cuanto a la realización de copias de seguridad del sistema de información	-Realizar pruebas al Módulo de Historia Clínica del Sistema de Información en cuanto a las Copias de Seguridad	

GA. 10	20/05/15	Verificación de la existencia de seguros que se adquieren para cada uno de los equipos del Área de Consulta Externa	-Solicitar la Información pertinente. -Aplicar lista de chequeo	
GA. 12	21/05/15	Aplicar las pruebas pertinentes en el Sistema de Información del Área de Consulta Externa	-Realizar el diseño y aplicación de las pruebas al Sistema de Información del Módulo de Historia Clínica del área de Consulta Externa	
GA. 13	26/05/15	Organización y análisis de la información recopilada.	-Reunir todos los soportes y documentación recogida durante la auditoria.	
GA. 14	27/05/15	Realización del dictamen.	-Reunir todos los hallazgos encontrados y proponer las posibles soluciones.	
GA. 15	01/06/15	Entrega del dictamen.	-Entregar el dictamen final.	

Fuente: Autores del proyecto

4.2.4 Inventario de software

La IPS Dr. Prosalud S.A.S. no tenía físicamente el inventario de software de los equipos correspondientes al proceso de consulta externa, por tal motivo el equipo auditor realizo el respectivo levantamiento de la información

DD	MM	AA
04	05	15

EMPRESA: IPS DR PROSALUD S.A.S
PERIODO: Del 01 al 31 DE MAYO 2015
RESPONSABLE: LUIS ENRIQUE LOPEZ
AREA AUDITADA: Consulta Externa

Ref.	Software	Versión	Núm. Inventario	Licencias	Presentación	Asignado a	Localización
W01	Windows	7	01 0012–1	1	CD-ROM	Consulta Externa	CE 01
W02	Windows	7 Pro	01 0012-2	2	CD-ROM	Consulta Externa	CE 02-03
W03	Windows	8	01-0013-1	3	CD-ROM	Consulta Externa	CE 04-07
W04	Windows	8 Pro	01-0013-2	2	CD-ROM	Recepción	SCE 01-02
W05	Office	2010	01-0014-1	4	CD-ROM	Consulta Externa	CE 01-04
W06	Office	2006	01-0014-2	2	CD-ROM	Recepción	SCE 01
W07	Norton Simantec Security	19.6.2	01-0015-1	10	CD-	Gerencia	JS 03-JS 13

Fuente: Autores del proyecto

4.2.5 Inventario de Hardware

La IPS Dr. Prosalud S.A.S. no tenía físicamente el inventario de hardware de los equipos correspondientes al proceso de consulta externa, por tal motivo el equipo auditor realizo el respectivo levantamiento de la información

DD	MM	AA
04	05	15

EMPRESA: IPS DR PROSALUD S.A.S
PERIODO: Del 01 al 31 DE MAYO 2015
RESPONSABLE: LUIS ENRIQUE LOPEZ
AREA AUDITADA: Consulta Externa

Núm.	Equipo	Marca	Núm. Inventario	Características	Observaciones
2	Computador	ACER	CE-0001-2		
1	Computador	LENOVO	CE-0003		
1	Computador	HP	CE-0004		
2	Procesador	Duo 2.40Ghz		Intel Celeron	
1	Procesador	CPU G1840		Intel Celeron	
1	Procesador	CPU G1610		Intel Celeron	
4	Mother Board	Asrok			
4	Memoria Ram 2Gb	Markvision			
4	Mouse	HP			
1	Router	TP-Link			

Fuente: Autores del proyecto

4.2.6 Desviaciones encontradas

Luego de realizado el levantamiento de la información y la aplicación de los instrumentos de recolección de información a los empleados del proceso de Consulta Externa de la IPS Dr. Prosalud S.A.S. se encontraron las siguientes desviaciones:

Fecha	04	05	2015
Nombre de la Empresa	DR PROSALUD IPS S.A.S.		
Área Auditada	Consulta Externa		

Ref.	Situaciones	Causas	Solución
DE-01	Se evidencia que en las instalaciones no hay alarmas y cámaras de seguridad dentro y fuera	En el momento no se considera importante el uso de estos elementos de	Se requiere instalar medios para proveer seguridad en especial en las áreas donde se

	de las instalaciones,	seguridad física.	procesa información.
DE-02	Se evidencia que en el área de recepción donde se encuentra el servidor no hay ningún control en el ingreso de visitantes. Así mismo tampoco hay avisos donde se restringa el acceso. .	No existe un área determinada para realizar esta labor.	Reubicar las instalaciones físicas del área donde se encuentra el servidor a un área independiente donde permita tener un control para realizar y resguardar la información
DE-03	Se evidencia la falta de políticas de seguridad y plan de contingencia de la dependencia.	No se tienen documentado los procesos.	Se recomienda la implementación de las políticas de seguridad y plan de contingencia
DE-04	Se evidenció que el servidor es de uso público, no hay control de accesos ni de seguridad.	Negligencia del jefe de procesos.	Se requiere ubicar el servidor en un instalación física independiente y segura, que brinde las condiciones físicas y lógicas
DE-05	Se evidenció que no hay personal encargado de las copias de seguridad, y desconocen quien y en donde es resguardada la información	Negligencia del Jefe de Procesos	Se requiere crear un manual de todo el proceso de realización de las copias de seguridad y la restauración de las mismas al igual la designación del personal encargado.

Fuente: Autores del proyecto

4.2.7 Situaciones encontradas

Seguido de enunciadas las desviaciones encontradas en el proceso de consulta externa de la IPS Dr. Prosalud S.A.S. se menciona a continuación las situaciones encontradas durante el proceso de recolección de información

Fecha	04	05	2015

Nombre de la Empresa	DR PROSALUD IPS S.A.S.
Área Auditada	Consulta Externa

Ref.	Situaciones	Causas	Solución	Responsable
SE-01	Se evidencia que en las instalaciones no hay alarmas y cámaras de seguridad dentro y fuera de las instalaciones,	En el momento no se considera importante el uso de estos elementos de seguridad física.	Se requiere instalar medios para proveer seguridad en especial en las áreas donde se procesa información.	Líder del proceso
SE-02	Se evidencia que en el área de recepción donde se encuentra el servidor no hay ningún control en el ingreso de visitantes. Así mismo tampoco hay avisos donde se restringa el acceso. .	No existe un área determinada para realizar esta labor.	Reubicar las instalaciones físicas del área donde se encuentra el servidor a un área independiente donde permita tener un control para realizar y resguardar la información	Líder del proceso
SE-03	Se evidencia la falta de políticas de seguridad y plan de contingencia de la dependencia.	No se tienen documentado los procesos.	Se recomienda la implementación de las políticas de seguridad y plan de contingencia	Líder del proceso
SE-04	Se evidenció que el servidor es de uso público, no hay control de accesos ni de seguridad.	Negligencia del jefe de procesos.	Se requiere ubicar el servidor en un instalación física independiente y segura, que brinde las condiciones físicas y lógicas	Líder del proceso

Fuente: Autores del proyecto

4.2.8 Situaciones relevantes

Dentro los desviaciones y situaciones encontradas en el proceso de consulta externa de la IPS Dr. Prosalud SA.S. se determinaron las siguientes situaciones relevantes:

Fecha	04	05	2015

Nombre de la Empresa	DR PROSALUD IPS S.A.S.
Área Auditada	Consulta Externa

Ref.	**Situaciones**	**Causas**	**Solución**
SR-01	Se evidencia que en el área de recepción donde se encuentra el servidor no hay ningún control en el ingreso de visitantes. Así mismo tampoco hay avisos donde se restringa el acceso. .	No existe un área determinada para realizar esta labor.	Reubicar las instalaciones físicas del área donde se encuentra el servidor a un área independiente donde permita tener un control para realizar y resguardar la información
SR-02	Se evidenció que el servidor es de uso público, no hay control de accesos ni de seguridad.	Negligencia del jefe de procesos.	Se requiere ubicar el servidor en un instalación física independiente y segura, que brinde las condiciones físicas y lógicas
SR-03	Se evidenció que no hay personal encargado de las copias de seguridad, y desconocen quien y en donde es resguardada la información	Negligencia del Jefe de Procesos	Se requiere crear un manual de todo el proceso de realización de las copias de seguridad y la restauración de las mismas al igual la designación del personal encargado.

Fuente: Autores del proyecto

4.2.9 Pruebas y resultados

En el desarrollo y ejecución de los instrumentos de recolección de información se encontraron varias falencias que llevo al equipo auditor a realizar las pruebas que se mencionan abajo en cada proceso que presentaba fallas en la información dada por los directivos y empleados del proceso de consulta externa de la IPS Dr. Prosalud.

Prueba No.01

Fecha	**04**	**05**	**2015**

Nombre de la empresa	DR PROSALUD IPS S.A.S.		
Área auditada	Consulta Externa		
Prueba	Realizar inventario del hardware		
Objetivo de la prueba	Evaluar posibles cambios o perdidas de hardware		
Tipo de prueba	**C** _____	**S** _____	**DF** ___X___
Procedimiento a emplear	Elaborar un listado de cada equipo, marca, modelo, N° de Inventario, Características y alguna observación adicional		
Recursos	Recursos humanos, tecnológicos, papelería.		
Resultados de la prueba			
Hallazgos	Se evidenció que los equipos no se encuentran inventariados.		
Causa	No se le ha dado importancia al inventario tecnológico ni mucho menos a la información que se maneja en el área.		
Situación de riesgo que genera	Daño físico o pérdida de las computadoras, equipo periférico y medios de comunicación. Los datos y programas almacenados en los chips de memoria de una computadora se pierden, robo de la información		
Recomendaciones de auditoria	Se debe tener un inventario físico tecnológico asignado a cada dependencia, ya que es de vital importancia porque ahí se encuentra toda la información		
Elaborado por	**Juais Celedon Alarcon**		
Revisado por	**Ober Alfredo Ruiz Daza**		

Fuente: Autores del proyecto

Prueba No. 02

Fecha	**15**	**05**	**2015**

Nombre de la empresa	DR PROSALUD IPS S.A.S.		
Área auditada	Consulta Externa		
Prueba	Verificar las políticas de seguridad física del Área Consulta Externa		
Objetivo de la prueba	Verificar la existencia de políticas de seguridad		
Tipo de prueba	**C** _____	**S** _____	**DF** ___X___
Procedimiento a emplear	Revisión de las políticas de seguridad definidas por la empresa.		
Recursos	Humanos, tecnológicos, documentación		
Resultados de la prueba			
Hallazgos	Se verifico que el área no cuenta con una política de seguridad documentada.		
Causa	Se tiene desconocimiento de la gran importancia que tiene la dependencia en la implementación de una política de seguridad con el fin de salvaguardar la información confidencial o vulnerable		
Situación de riesgo que genera	Acceso, uso, divulgación, daño e interferencia de la información.		
Recomendaciones de auditoria	Se recomienda la implementación de las políticas de seguridad basadas en normas ISO/IEC 27000 series		
Elaborado por	**Juais Celedon Alarcon**		
Revisado por	**Ober Alfredo Ruiz Daza**		

Fuente: Autores del proyecto

Prueba No.03

Fecha	15	05	2015

Nombre de la empresa	DR PROSALUD IPS S.A.S.		
Área auditada	Consulta Externa		
Prueba	Verificación de niveles de acceso de los usuarios en el Sistema de Información.,		
Objetivo de la prueba	Determinar los controles acceso lógico para restringir el acceso a la información sensible del área de Consulta Externa.		
Tipo de prueba	**C** _____	**S** ___X___	**DF** _____
Procedimiento a emplear	Ingresar al Área de Consulta Externa. Verificar la ausencia del médico tratante en cada estación de trabajo del área de Consulta externa. Ingresar al equipo de cómputo.		
Recursos	Recurso humano y tecnológico.		
Resultados de la prueba			
Hallazgos	Se evidencio que las estaciones de trabajo están bloqueadas en ausencia del médico tratante en el área de Consulta Externa mediante contraseñas.		
Causa			
Situación de riesgo que genera	Daño o perdida de la información		
Recomendaciones de auditoria			
Elaborado por	**Juais Celedon Alarcon**		
Revisado por	**Ober Alfredo Ruiz Daza**		

Fuente: Autores del proyecto

Prueba No.04

Fecha	**15**	**05**	**2015**

Nombre de la empresa	DR PROSALUD IPS S.A.S.		
Área auditada	Consulta Externa		
Prueba	Verificación de niveles de acceso de los usuarios en el Sistema de Información.,		
Objetivo de la prueba	Determinar los controles acceso lógico para restringir el acceso a la información sensible del área de Consulta Externa.		
Tipo de prueba	**C** _____	**S** ___X___	**DF** _____
Procedimiento a emplear	Ingresar al Área de Consulta Externa. Verificar la ausencia del médico tratante en cada estación de trabajo del área de Consulta externa. Ingresar al equipo de cómputo.		
Recursos	Recurso humano y tecnológico.		
Resultados de la prueba			
Hallazgos	Se evidencio que las estaciones de trabajo están bloqueadas en ausencia del médico tratante en el área de Consulta Externa mediante contraseñas.		
Causa			
Situación de riesgo que genera	Daño o perdida de la información		
Recomendaciones de auditoria			
Elaborado por	**Juais Celedon Alarcon**		
Revisado por	**Ober Alfredo Ruiz Daza**		

Fuente: Autores del proyecto

PRUEBA No.05

Fecha	**12**	**05**	**2015**

Nombre de la empresa	DR PROSALUD IPS S.A.S.		
Área auditada	Consulta Externa		
Prueba	Verificar el ingreso de datos al Sistema de Información.,		
Objetivo de la prueba	Determinar las fallas del personal en el manejo del módulo Historia Clínica en el área de Consulta Externa		
Tipo de prueba	**C** _____	**S** _____	**DF** ___X___
Procedimiento a emplear	Ingresar al Área de Consulta Externa. Ingresar al Sistema de Información Ingresar al Módulo de Consulta Externa Verificación de los datos a ingresar en el módulo de Historia Clínica		
Recursos	Recurso humano y tecnológico.		
Resultados de la prueba			
Hallazgos	Se evidencio que el personal Médico no ingresa todos los datos en el Modulo Historia Clínica		
Causa	El Médico tratante no conoce el módulo de Historia Clínica y a su vez no pregunta al paciente toda la información preliminar		
Situación de riesgo que genera	Daño o perdida de la información		
Recomendaciones de auditoria	Realizar jornadas de capacitación al personal Médico Tratante en el uso y manipulación del Módulo de Historia Clinica		
Elaborado por	**Juais Celedon Alarcon**		
Revisado por	**Ober Alfredo Ruiz Daza**		

Fuente: Autores del proyecto

Prueba No.06

Fecha	**19**	**05**	**2015**

Nombre de la empresa	DR PROSALUD IPS S.A.S.		
Área auditada	Consulta Externa		
Prueba	Analizar los procedimientos para la realización de las copias de seguridad.		
Objetivo de la prueba	Determinar mecanismos para salvaguardar la información del área de consulta externa		
Tipo de prueba	**C** _____	**S** ___X___	**DF** _____
Procedimiento a emplear	Ingresar al Servidor. Revisar que Software maneja el área para resguardar la información Verificar donde son almacenadas las Copias de Seguridad. Revisar el mecanismo de protección de la información. Verificar el personal responsable de salvaguardar la información.		
Recursos	Recurso humano y tecnológico.		
Resultados de la prueba			
Hallazgos	Se evidenció que el proceso de copias de seguridad se hace en un computador normal, que a su vez es utilizado en el área de recepción. El computador no cuenta con un regular de voltaje (UPS) Las copias de seguridad quedan ubicadas en el disco duro no se realiza una copia en un disco externo. No hay personal encargado para realizar copias de seguridad se generan automáticamente. La entidad que vendió el Sistema de Información genera mensual copias de seguridad que reposan en sus servidores.		
Causa	No se definieron políticas de seguridad y/o confidencialidad en el momento de la adquisición del Sistema de Información. No se adquirió equipos tecnológicos para salvaguardar la información.		
Situación de riesgo que genera	Daño o perdida de la información		
Recomendaciones de auditoria	Crear una espacio físico independiente para el área del servidor Adquirir infraestructura tecnológica adecuada para los requerimientos de respaldo de información Contratar una persona que se le asigne la administración del Sistema de Información, que brinde soporte ante cualquier evento.		
Elaborado por	**Juais Celedon Alarcon**		
Revisado por	**Ober Alfredo Ruiz Daza**		

Fuente: Autores del proyecto

4.2.10 Dictamen

Después del análisis realizado de la información recolectada y las pruebas realizadas el equipo auditor realizo el siguiente informe ejecutivo entregado a la junta de socios junto al legajo de trabajo.

Ocaña, 1 de Junio de 2015

Doctor
DORIAN ENRIQUE RIVERA
Gerente General
DR PROSALUD IPS S.A.S
E.S.D

Cordial saludo:

De acuerdo a la inquietud manifestada por usted para evaluar el correcto funcionamiento en el área de Consulta Externa de la empresa DR PROSALUD IPS S.A.S, me dirijo a usted presentándole el dictamen de la auditoria enfocada en la realización de copias de seguridad de dicha dependencia llevada a cabo del 27 de Abril al 01 de Junio de 2015.

Mediante los resultados obtenidos durante la evaluación me permito informarle que el computador donde se realiza las copias de seguridad no cuenta con un regulador de voltaje (UPS) ocasionando pérdidas de datos al presentarse una falla eléctrica; de igual forma para el proceso de realización de copias de seguridad no se cuenta con una persona encargada, este proceso se ejecuta en el computador que utiliza la recepción lo que puede originar daños por virus o que accidentalmente se interrumpa o se elimine dicho proceso. Así mismo, las copias de seguridad generadas hasta el momento son almacenadas en el mismo disco duro del computador de recepción sometiendo la información a daño, pérdida o robo.

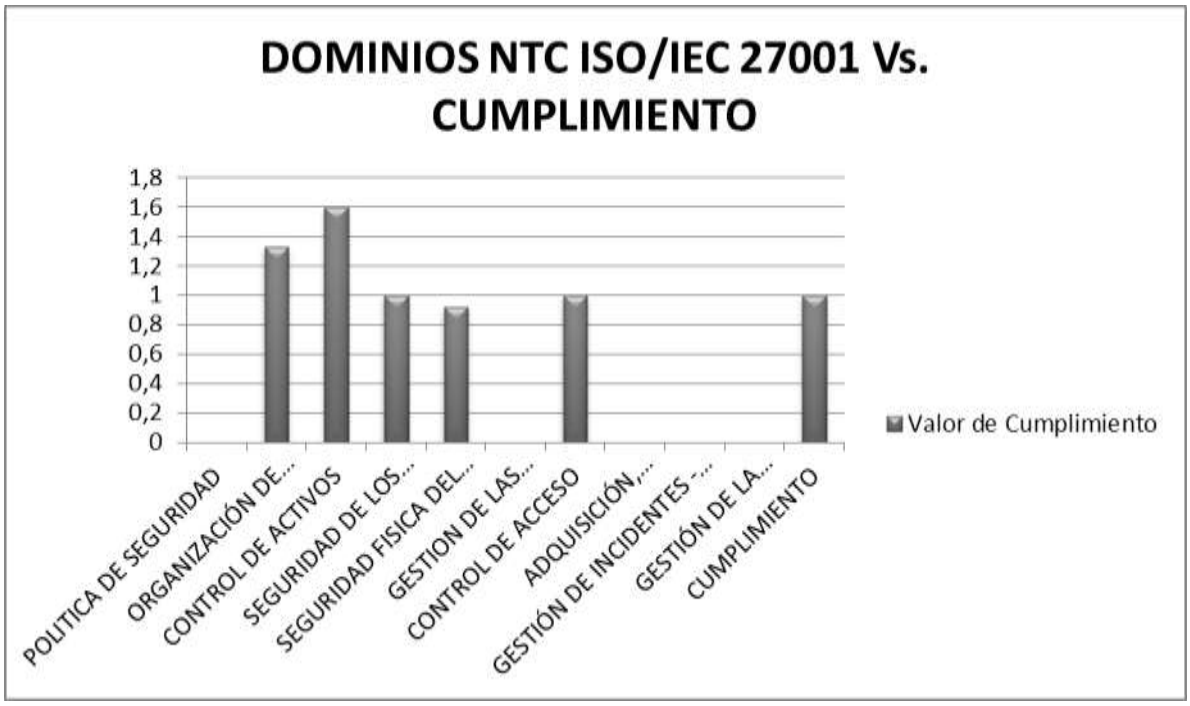
De acuerdo con las pruebas realizadas en el Área de Consulta Externa me permito dictaminar que en la empresa DR PROSALUD IPS S.A.S se debe crear un espacio físico independiente para el área del servidor y a su vez contratar una persona interna que se le asigne la administración del Sistema de Información, que brinde soporte ante cualquier evento, así mismo se sugiere adquirir infraestructura tecnológica adecuada para los requerimientos de respaldo de información.

Atentamente,

Equipo Auditor

4.2.11 Evaluación de Controles al proceso de Consulta Externa de la IPS Dr. Prosalud S.A.S. basada en NTC-ISO-IEC-27001

Se realizó una evaluación de la norma NTC ISO/IEC 27001 solo para el proceso de consulta externa de la IPS Dr. Prosalud S.A.S.; así como se muestra en el Anexo teniendo en cuenta los controles que se intervienen arrojándonos el siguiente gráfico:



Fuente: Autores del proyecto

Se puede observar en el grafico anterior que el nivel de cumplimiento en la mayoría de los dominios no cumplen con los controles asociados; asi mismo los dominios gestión de las comunicaciones y operaciones; adquisición, desarrollo y mantenimiento de sistemas de información; gestión de incidentes-monitoreo y gestión de continuidad del negocio no se tuvieron en cuenta dentro del proceso de consulta externa. El porcentaje que nos arroja en el nivel de cumplimiento de la norma NTC/IS0 27001 es del 22% el cual nos muestra el estado en el que se encuentra la información en la organización.

4.3 GUÍA DE GESTIÓN DE RIESGOS COMO APOYO A LA SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE CONSULTA EXTERNA DE LA IPS DR PROSALUD S.A.S

4.3.1 Proposito de la guía de gestión de riesgos. Esta guía se desarrolla con el fin de brindarle a la IPS Dr. Prosalud S.A.S. una herramienta confiable para la identificación, análisis y gestión de riesgos del proceso de consulta externa garantizando el cumplimiento de sus objetivos estratégicos.

4.3.2 Alcance de la guía de gestión de riesgos. Esta guía se realiza para el proceso y los subprocesos de consulta externa de la IPS Dr. Prosalud S.A.S, el cual nos proporcionan toda la información necesaria para identificar, analizar y evaluar los riesgos y proporcionar mejoras, realizando asi una gestión de estos riesgos dentro de la IPS Dr. Prosalud.

Para aplicar la norma NTC-ISO31000, se inicia desde el establecimiento del contexto, realizando la valoración del riesgo y las actividades que se encuentre incluidas dentro de la misma (identificación, análisis y evaluación) y parte del tratamiento que está comprendido como la generación de recomendaciones; la determinación de que controles se debe aplicar depende de la alta gerencia y según como lo considere pertinente.

4.3.3 Usuarios de la guía de gestión de riesgos. Esta guía está enfocada a las personas que están involucradas en el proceso de consulta externa de la IPS Dr. Prosalud S.A.S entre ellos están el gerente de la organización, el subgerente científico quienes evalúan los riesgos y el personal médico que son quienes identifican los riesgos dentro de los procesos que ejecutan.

4.3.4 Objetivo de la guía de gestión de riesgos. Implantar en los procesos y subprocesos de consulta externa en la IPS Dr. Prosalud S.A.S. la gestión del riesgos.

4.3.5 Guía de Aplicación de la norma. Según la norma NTC-ISO 31000, su aplicación para la IPS Dr. Prosalud S.A.S. para el proceso de consulta externa, se realizaría aplicando la siguiente guía:

Establecimiento del contexto. Es el conjunto de circunstancias que rodean y condicionan la gestión del riesgo tanto interna como externamente.

Contexto interno. Este contexto es el ambiente interno en el cual la organización busca alcanzar sus objetivos. Se establece la misión, visión y objetivos de la organización, las políticas que están implementadas, la cultura de la misma, su estructura y estrategia y todo lo que afecte el funcionamiento interno de la misma.

FACTORES INTERNOS	DESCRIPCION
Personal	Empleados que trabajan en el área de consulta externa.
Recursos	Equipos de cómputo y comunicaciones.
Economía	Influye en el proceso al capital para inversión y adquisición de nuevas tecnologías.

Fuente: Autores del Proyecto

Contexto externo. En este contexto se establece las normas vigentes que apliquen a la organización según su actividad económica, las políticas públicas, la demografía, el comercio, la tecnología, y todo aquello que tiene relación con la compañía desde un ambiente externo y que afecte su funcionamiento.[16]

FACTORES EXTERNOS	DESCRIPCION
Clientes	Personas que solicitan el servicio.
Tecnología	Se refiere al proceso de actualización de hardware y software.
Proveedores	Personas que vendieron el software a la IPS.

Fuente: Autores del Proyecto

Contexto del proceso para la gestión del riesgo. En esta parte se deben especificar hasta donde va a llegar la gestión del riesgo en el proceso o área seleccionada, se define las metas, objetivos, responsabilidades, alcance, profundidad y extensión, relación con los otros procesos, metodología, forma de evaluar el desempeño y eficacia de la gestión.

Definir los criterios de riesgo. Como se mencionó anteriormente se tienen en cuenta dos aspectos: la probabilidad y el impacto; la probabilidad tiene los criterios para la evaluación del riesgo mostrados a continuación:

NIVEL	CONCEPTO	DESCRIPCION
1	Insignificante	Afectaría el desarrollo de tareas, actividades y procedimientos.
2	Menor	Afectaría el desarrollo de otros procesos institucionales.
3	Moderado	Generaría paro intermitente del proceso.
4	Mayor	Generaría el paro total del proceso.
5	Catastrófico	Generaría el paro total de la entidad.

Fuente: YENIS PIEDAD OSORIO RIVERO, YESICA MARÍA PÉREZ PÉREZ. DISEÑO DE UNA POLÍTICA DE GESTIÓN DE RIESGOS DE LA INFORMACIÓN PARA LA DEPENDENCIA DE ADMISIONES REGISTRO Y CONTROL DE UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. Autor: Tesis de grado para la Esp Auditoria de Sistemas, 2014

El impacto tiene los criterios para la evaluación del riesgo mostrados a continuación:

[16] http://tienda.icontec.org/brief/NTC-ISO31000.pdf

NIVEL	CONCEPTO	DESCRIPCION
A	Casi Certeza	Se espera que ocurra en la mayoría de las circunstancias
B	Probable	Probablemente ocurrirá en la mayoría de las circunstancias
C	Posible	Podría ocurrir en algún momento.
D	Improbable	Pudo ocurrir en algún momento.
E	Raro	Puede ocurrir solo en circunstancias excepcionales.

Fuente: YENIS PIEDAD OSORIO RIVERO, YESICA MARÍA PÉREZ PÉREZ. DISEÑO DE UNA POLÍTICA DE GESTIÓN DE RIESGOS DE LA INFORMACIÓN PARA LA DEPENDENCIA DE ADMISIONES REGISTRO Y CONTROL DE UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA. Autor: Tesis de grado para la Esp Auditoria de Sistemas, 2014

4.3.6 Valoración del riesgo. La valoración del riesgo está basada en dos aspectos generalmente usados para este fin, la probabilidad que es la oportunidad que algo suceda[17] como la cantidad de veces que se puede repetir el riesgo e impacto como las consecuencias que implica en la empresa la materialización del riesgo, es decir los daños causados después de realizado el riesgo.

Identificación del riesgo. La identificación es el paso más importante para la gestión de riesgos ya que el riesgo que no se identifique en este punto, no será tenido en cuenta en el análisis posterior y por lo tanto no será evaluado.

NOMBRE DEL PROCESO	Consulta Externa
OBJETIVO DEL PROCESO	Describir los diferentes procedimientos básicos para el subproceso establecido para realizar la atención de un usuario en el servicio de consulta externa

NO.	CAUSAS (FACTORES INTERNOS Y EXTERNOS)	RIESGO	DESCRIPCIÓN	EFECTO (CONSECUENCIA)	TIPO / IMPACTO
	Los proveedores no ofrezcan la ultima versión del	Desactualización del software	Sin un adecuado software estamos expuestos a	Atraso en la obtención de datos e indicadores. Pérdida de información.	Operativo Cumplimien

[17] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del Riesgo. Principios y Directrices. Bogotá D.C.: ICONTEC, 2011.NTC ISO 31000.

1	SI. No haya disponibilidad de inversión en tecnología.		retrocesos de tipo administrativo y asistencial, tales como: Mala facturación, mal descripción de procedimientos asistenciales, problemas con radicación de cuentas, problemas con cobro de cartera, problemas con el cálculo de costos.	Falta de credibilidad. Menos argumentos para tomas de decisiones por parte de la alta gerencia.	to Estratégico Imagen Tecnología
2	Falla eléctricas Fallas en los equipos de computo y comunicación.	Perdida y/o robo de la información	Estamos expuestos al plagio de la información, lo cual nos puede llevar a consecuencias de tipo penal y administrativo y a retrocesos de procesos de mejoramiento continuo de la calidad.	Entrega de indicadores a tiempo. No hacer análisis de la información. Imposibilidad de hacer tomas de decisiones a tiempo basada en hechos reales.	Operativo Cumplimiento Estratégico Imagen Tecnología
3	No hay buena retribución monetaria por obra o labor.	Rotación frecuente del personal	Traumatismo en la producción y análisis de indicadores	Demoras en la entrega de informes. Pérdida de tiempo en procesos de capacitación.	Operativo Cumplimiento Estratégico Imagen Tecnología
4	Perdida de la	Influencia para	Utilización del	Inconformismo de	

	información de la asignación de citas. Servidor Apagado.	la consecución de citas médicas.	poder que confiere un alto cargo y omitir los trámites correspondientes para el otorgamiento de citas médicas, favoreciendo a familiares y amigos.	los usuarios. Limitación en la contratación con las EPS por las barreras a la asignación de citas. Quejas de los usuarios ante las entidades correspondientes. Desmotivación y malestar de los usuarios en seguir el procedimiento para conseguir una cita. Enfrentamientos internos entre el usuario y funcionarios.	Operativo Cumplimiento Estratégico Imagen Tecnología
5	Falla en el fluido eléctrico. Servicio de Red. Servidor apagado (proveedor)	Perdida de soportes de historia clínica o de las Historias Clínicas.	Manejo indebido de Historias Clínicas de los usuarios e información contenida en ellas, que por su carácter reservado debe ser de exclusivo acceso a determinados funcionarios.	Posibles demandas judiciales contra la entidad. Traumatismos en el proceso de atención al usuario. Detrimento de la imagen institucional. Pérdida de la cita médica, solicitada por el usuario.	Operativo Cumplimiento Estratégico Imagen Tecnología
6	Contratación con personal médico especializado. Numero de citas restringidas	Retrasos en la programación de citas especialistas	Elevados tiempos de espera para la inclusión de los pacientes en lista para citas especialistas	Deterioro del estado de salud de los pacientes Tramitología ante la EPS Falta de información precisa al usuario. Autorización de las	Operativo Cumplimiento Estratégico Imagen Tecnología

				EPS para otras IPS que garanticen mayor oportunidad.	
7	No están delimitadas las áreas. Los equipos de cómputo no están en un lugar seguro. No hay equipos de video-vigilancia.	Inseguridad en el área.	La falta de vigilancia, iluminación en pasillos y buenas cerraduras en las puertas y ventanas, hacen del área un sitio inseguro para la prestación del servicio.	Pérdida de materiales e instrumentos de uso médico para el servicio de los usuarios. Dificultas para la prestación de un buen servicio. Pérdidas económicas para la IPS. Se crea un ambiente de desconfianza entre los funcionarios del área.	Operativo Cumplimiento Estratégico Tecnología

Fuente: Autores del Proyecto

Análisis del riesgo. Para realizar el análisis del riesgo debemos primero entenderlo, es decir validar si es inevitable tratarlos y determinar cuáles son las estrategias adecuadas que debe implementar la IPS Dr. Prosalud S.A.S. Para ello se debe considerar las causas y la fuente del riesgo, sus consecuencias positivas y negativas, y la probabilidad de que tales consecuencias puedan ocurrir.[18]

Al impacto y la probabilidad identificada, se le debe realizar un análisis, el cual puede ser cualitativo, semicuantitativo, cuantitativo o una combinación de ellos.

✓ Análisis cualitativo, utiliza palabras para describir la magnitud de las consecuencias potenciales y la posibilidad de que ocurran tales consecuencias.

✓ Análisis semicuantitativo, se dan en valores y el objetivo es producir una escala de clasificación más amplia que la que se obtiene usualmente en el análisis cualitativo, sin sugerir valores realistas para riesgos.

✓ Análisis cuantitativo, utiliza valores numéricos, tanto para las consecuencias como para la posibilidad, empleando datos provenientes de una variedad de fuentes[19]

[18] Ibíd. NTC/ISO 31000.
[19] Ibíd. NTC/ISO 31000.

Según nuestro análisis nos arroja el siguiente:

NOMBRE DEL PROCESO	Consulta Externa
OBJETIVO DEL PROCESO	Describir los diferentes procedimientos básicos para el subproceso establecido para realizar la atención de un usuario en el servicio de consulta externa

NO	**RIESGO**	**CLASIFICACION DEL RIESGO**				
		PROBABILIDAD		**IMPACTO**		**VALOR**
1	Desactualización del software	c	Posible	4	Mayor	C4
2	Perdida y/o robo de la información	c	Posible	5	Catastrofico	C5
3	Rotación frecuente del personal	c	Posible	4	Mayor	C4
4	Influencia para la consecución de citas médicas.	C	Posible	3	Moderado	C3
5	Perdida de soportes de historia clínica o de las Historias Clínicas.	C	Posible	5	Catastrófico	C5
6	Retrasos en la programación de citas especialistas	D	Improbable	1	Insignificante	D1
7	Inseguridad en el área.	C	Posible	3	Moderado	C3

Fuente: Autores del Proyecto

Evaluación del Riesgo. El propósito de la evaluación del riesgo es tomar decisiones, basadas en los resultados del análisis del riesgo, sobre los riesgos que necesitan tratamiento y las prioridades del tratamiento[20].

Se deben considerar los objetivos a cumplir dentro de la organización y para nuestro caso dentro de los procesos de consulta externa, con el fin de alinearlos a la oportunidad que podría generarse al realizar esta evaluación.

[20] Ibid. NTC/ISO 31000.

Se tendrá en cuenta la siguiente matriz para la valoración del riesgo

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E
B: Zona de riesgo baja: Asumir el riesgo M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir					

Fuente: Guia de Riesgos DAFP

NOMBRE DEL PROCESO		Consulta Externa						
OBJETIVO DEL PROCESO		Describir los diferentes procedimientos básicos para el subproceso establecido para realizar la atención de un usuario en el servicio de consulta externa						
NO	**RIESGO**	**CLASIFICACION DEL RIESGO**					**EVALUACION DEL RIESGO**	
		PROBABILIDAD		**IMPACTO**		**VALOR**		
1	Desactualización del software	c	Posible	4	Mayor	C4	2	Zona Riesgo Extrema
2	Perdida y/o robo de la información	c	Posible	5	Catastrofico	C5	2	Zona Riesgo Extrema
3	Rotación frecuente del personal	c	Posible	4	Mayor	C4	2	Zona Riesgo Extrema
4	Influencia para la consecución de citas médicas.	C	Posible	3	Moderado	C3	1	Zona Riesgo Alta
5	Perdida de soportes de historia clínica o de las Historias Clínicas.	C	Posible	5	Catastrófico	C5	2	Zona Riesgo Extrema
6	Retrasos en la programación de citas especialistas	D	Improbable	1	Insignificante	D1	3	Zona Riesgo Moderada
7	Inseguridad en el área.	C	Posible	3	Moderado	C3	4	Zona Riesgo Alta

Fuente: Autores del Proyecto

Tratamiento del Riesgo. El tratamiento de los riesgos está basado en la identificación de los mejores métodos definidos, para tomar una decisión sobre cada uno de estos teniendo en cuenta una serie de aspectos lo cuales a continuación mencionamos:

✓ **Aceptar:** Significa que no se toman medidas relativas con un riesgo de T.I particular, y la pérdida es aceptada si se produce. A diferencia de ignorar el riesgo, aceptar el riesgo supone que el riesgo es conocido; es decir, es una decisión informada y se ha aceptado por los directivos de la institución.

✓ **Transferir:** Significa reducir la probabilidad del riesgo o su impacto mediante la transferencia o distribución de una parte del riesgo. Las técnicas más comunes es adquirir seguros o realizar tercerizaciones (outsourcing) para tratar el riesgo.

✓ **Mitigar:** Significa que están siendo tomadas medidas para detectar el riesgo, seguido por la definición de una acción y unos controles para reducir la probabilidad y/o el impacto de un riesgo de T.I.

✓ **Evitar:** Evitar significa no permitir la ejecución de las actividades o de las condiciones que dan lugar a riesgo de T.I. Esta categoría se aplica cuando no hay otra respuesta adecuada al riesgo debido a su costo o impacto.

NOMBRE DEL PROCESO			Consulta Externa								
OBJETIVO DEL PROCESO			Describir los diferentes procedimientos básicos para el subproceso establecido para realizar la atención de un usuario en el servicio de consulta externa								
NO	**RIESGO**	**CLASIFICACION DEL RIESGO**					**EVALUACION DEL RIESGO**		**MEDIDA DE RESPUESTA**	**CONTROL**	**RESPONSABLE**
		PROBABILIDAD		**IMPACTO**		**VALOR**					
1	Desactualización del software	C	Posible	4	Mayor	C4	2	Zona Riesgo Extrema	Reducir el riesgo, evitar, compartir o transferir	Adquirir la actualización de software en la medida de las necesidades	Subdirección Administrativa Gerencia
2	Perdida y/o robo de la información	C	Posible	5	Catastrofico	C5	2	Zona Riesgo Extrema	Reducir el riesgo, evitar, compartir o transferir	Hacer gestión de los datos Estandarizar la información. Crear políticas de confidencialidad y respeto en la difusión de la información.	Gerencia Todas las Areas
3	Rotación frecuente del	C	Posible	4	Mayor	C4	2	Zona Riesgo	Reducir el riesgo,	Verificar la idoneidad del personal, a través de la	Gerencia Subdirecc

	personal							Extrema	evitar, compartir o transferir	gestión del talento humano. Evaluar las competencias del personal Garantizar la estabilidad del personal	ión Administrativa
4	Influencia para la consecución de citas médicas.	C	Posible	3	Moderado	C3	1	Zona Riesgo Alta	Reducir el riesgo, evitar, compartir o transferir	Realizar y establecer un manejo generalizado para ayudar a la consecución de una cita médica, en donde no intervengan factores particulares. Hacer seguimiento en las áreas de Consulta Externa y Atención al Usuario, para verificar la imparcialidad en la prestación del servicio. Dar estricto cumplimiento al orden de las citas, exceptuando aquellas urgentes o de usuarios residentes fuera de la ciudad.	Personal de Consulta Externa Oficina atención al usuario Oficina de control interno
5	Perdida de soportes de historia clínica o de las	C	Posible	5	Catastrófico	C5	2	Zona Riesgo Extrema	Reducir el riesgo, evitar, compartir o	Restringir el acceso y manejo de historias clínicas y demás documentos a personas diferentes a las	Archivo Central Oficina

	Historias Clínicas.								transferir	autorizadas. Llevar registro diario de entrada y salida de historias clínicas, con la firma delos responsables y quienes tiene acceso a ella.	de Control Interno
6	Retrasos en la programación de citas especialistas	D	Improbable	1	Insignificante	D1	3	Zona Riesgo Moderada	Asumir el riesgo, reducir el riego	Campañas de citas especialistas represadas Actualización del proceso de programación de citas.	Enfermen jefe Oficina control interno
7	Inseguridad en el área.	C	Posible	3	Moderado	C3	4	Zona Riesgo Alta	Reducir el riesgo, evitar, compartir o transferir	Mayor seguridad en los consultorios. Llevar registro y control sobre la existencia de equipos entregados. Realizar periódicamente inventarios, informando oportunamente las anomalias	Subgerente Cientifico Recursos Humanos Control Interno Gerencia

Fuente: Autores del Proyecto

4.3.6.1 Monitoreo y revisión. Las actividades de monitoreo y revisión deben estar planificadas para la gestión del riesgo e incluir verificación y vigilancia regular.

Las responsabilidad del monitoreo y revisión estarán a cargo tal comose espeficio en el cuadro anterior con el fin de estar prestos a cualquier evento que suceda dentro de los procesos.

CONCLUSIONES

Con la implementación de varios artefactos de recolección de información en el área de Consulta Externa de la IPS Dr Prosalud S.A.S. se pudo percibir el estado en que se encontraba la entidad con respecto a la manipulación de su mejor activo, notando que no tenían una estructura organizacional específica para los procesos que se manejan en la entidad y haciendo una estructura real de sus recursos tecnológicos utilizados por ellos se logró construir un modelo del negocio que mejora la calidad de los servicios prestados.

También éste diagnóstico nos permitió descubrir las principales amenazas a que está siendo expuesta la información que se maneja en esta dependencia y utilizando buenas prácticas como NTC ISO 27001 y NTC ISO 27002, asociadas a las buenas prácticas de auditorías a redes y bases de datos, auditorías a adquisición de tecnología, sistemas operativos, auditoria y gestión de riesgos de TI, elaborando y aplicando algunos instrumentos de recopilación de información se pudo generar un informe de auditoría que mostró con más claridad las vulnerabilidades que presenta la IPS. Apoyados en el análisis de los resultados obtenidos y en los documentos y normas que más se asemejan a ésta investigación se pudo generar un dictamen de la auditoría realizada dando conocimiento a la directiva de la IPS Dr Prosalud S.A.S.

Como en la IPS Dr Prosalud S.A.S. no se tienen implementadas metodologías de gestión de riesgos, se buscó una que se pudiera adaptar al proceso de la IPS, dando pie a la creación de una guía de gestión de riesgos tecnológicos para la entidad, dentro del estudio realizado para la identificación de la norma se tuvo en cuenta ISO/IEC 27002, ISO 31000/2009 buscando mitigar los riesgos detectados hasta el momento. En el diseño de la presente guía, se aplicaron lineamientos de la norma ISO 31000/2009 donde se establece una serie de principios de carácter genérico, fundamentales que se deben cumplir para hacer una gestión eficaz de riesgo, conociendo el valor, la manipulación y el control de éstos de la dependencia de Consulta Externa de la IPS Dr Prosalud S.A.S mejorando y brindando controles evolutivos a los procesos y así contribuir en el cumplimiento de los objetivos institucionales de la IPS.

Con el estudio de la presente investigación se lograron los objetivos previstos dentro de las delimitaciones propuestas, esperando que pueda ser tenida en cuenta para futuras investigaciones y ampliar el campo de acción haciendo una mejora continua en los procesos de gestión del riesgo en las entidades públicas y privadas.

RECOMENDACIONES

Socializar el resultado de esta investigación con los funcionarios de consulta externa y con los directivos de la IPS Dr Prosalud S.A.S.

Capacitar al personal de la oficina y a todo funcionario que esté involucrado en el proceso de consulta externa a fin de generar cultura organizacional y preservar la información que ahí se maneja.

Establecer coordinaciones entre las diferentes dependencias de la IPS Dr Prosalud S.A.S. para la ejecución compartida de los acciones de reducción de riesgos de la información.

Implementar un sistema de gestión de riesgos de la información contemplando el diseño de la guía resultado de la presente investigación como parte activa de dicho sistema.

BIBLIOGRAFIA

ACOSTA PORTILLO. Dinael, ALVAREZ PRADA. Ingrid Lorena, CAMARGO BARBOSA. Jorge Alberto, NÚÑEZ ASCANIO. Karen Lorena. Diseño de un modelo de gestión del riesgo de tecnologías de información para la unidad de contabilidad de la universidad francisco de paula Santander [Libro]. - OCAÑA : Tesis de grado para la Esp Auditoria de Sistemas, 2013.

ARISTIZABAL. Edier, VARGAS. Richard, MESA. Oscar. Diagnóstico y propuesta para una gestión integral del riesgo en valle de aburrá, 2008.

G. GRANADOS PAREDES, «Introducción a la criptogragía,» Revista Digital Universitaria, vol. 7, nº 7, pp. 2-17, 2006.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI). Bogotá D.C.: ICONTENC, 2006. NTC ISO/IEC 27001.

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.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información. Bogotá D.C.: ICONTEC, 2009. NTC ISO/IEC 27005.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del Riesgo. Principios y Directrices. Bogotá D.C.: ICONTEC, 2011.NTC ISO 31000.

OSORIO RIVERO. Yenis piedad, PÉREZ PÉREZ. Yesica maría. Diseño de una política de gestión de riesgos de la información para la dependencia de admisiones registro y control de universidad francisco de paula Santander Ocaña. Autor: Tesis de grado para la Esp Auditoria de Sistemas, 2014

RAMÍREZ MUÑOZ. Jorge enrique. Análisis de evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la alcaldía de pamplona - Norte de Santander. Tesis de Grado para la Esp Seguridad Informática UNAD, 2015

REFERENCIAS DOCUMENTALES ELECTRONICAS

ARCE SANTOLAYA. Rubén. El diario de empresarios y directivos. [En línea]. Publicado en internet el 20 de marzo de 2015. Ubicado en la URL: http://diarioempresariosydirectivos.blogspot.com.co/2015/03/gestion-del-riesgo-en-los-proyectos.html

CARDONA. Omar Dario. La necesidad de repensar de manera holística los conceptos de vulnerabilidad y riesgo. Una crítica y una revisión necesaria para la gestión, critica a los diferentes enfoques".[En línea]. Ubicado en la URL: http://www.desenredando.org/public/articulos/2003/rmhcvr/rmhcvr_may-08-2003.pdf

Expense Reduction Analyst. Gestion de riesgos en la empresa. [En linea]. Publicado en internet en el año (2009-2016). Ubicado en la URL: http://expensereduction.eu/es/blog/gesti%C3%B3n-de-riesgos-en-la-empresa#.VhRx7_l_Oko

MEGA INTERNACIONAL. Administración de riesgos empresariales. [En línea]. Publicado en internet en el año 2015. Ubicado en la URL: http://www.mega.com/es/solucion/administracion-de-riesgos-empresariales

MINISTERIO DEL INTERIOR Y JUSTICIA. Mejora continua. [En línea]. Ubicado en el URL: https://www.mininterior.gov.co/sites/default/files/guia_2.pdf

NTC 5254. Fundamentos de la gestión de riesgo. [En línea]. Ubicado en la URL: http://www.pascualbravo.edu.co/pdf/calidad/gestionriesgos.pdf

PMBOOK GESTION. Riesgos. [En línea]. Ubicado en la URL: http://pmbok1.blogspot.com/p/blog-page_2251.html

ROLLING MEADOWS, IL, USA SACA. Publica en Español el Marco de Riesgos de TI para Ayudar a las Organizaciones a Obtener Beneficios y a Mitigar los Riesgos. [En línea]. Publicado en internet el 01 de Julio de 2010. Ubicado en la URL: http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Publica-en-Espa%C3%B1olel-Marco-de-RiesgosdeTIparaAyudaralasOrganizacionesa-Obtener-Beneficios-y-a-Mitigar-los-Riesgos.aspx

RAMIREZ MONTAÑEZ. Jorge enrique. Análisis, evaluación de riesgos y asesoramiento de la seguridad informática en el área de redes y sistemas de la alcaldía de pamplona - norte de Santander. [En línea]. Publicado en internet en el año 2015. Ubicado en la URL: http://hdl.handle.net/10596/3415 http://repository.unad.edu.co/handle/10596/3415

UNIDAD NACIONAL DE GESTIÓN DE RIESGOS DE DESASTRES. Glosario de términos de la gestión de riesgos de desastres. [En linea]. Publicado en internet en el año

2015. Ubicado en la URL: http://portal.gestiondelriesgo.gov.co/Paginas/Glosario_Terminos_Gestion_del_Riesgo.aspx

ANEXOS

ENTREVISTA AL JEFE DE AREA DE CONSULTA EXTERNA (SUBGERENTE CIENTIFICO)

Objetivo: Adquirir la información necesaria para comprender la estructura del Módulo Historia Clínica

1. ¿Existe un manual de Organización en donde se describan todos los procedimientos, normas y funciones que faciliten el desarrollo de la empresa?

2. ¿Los recursos con los que cuenta el área son los adecuados y suficientes para el óptimo desarrollo del proceso de Consulta Externa?

3. ¿La tecnología con la que cuenta el área de Consulta Externa es la apropiada para el desarrollo de sus actividades?

4. ¿En el momento de la adquisición del Sistema de información se realizó un estudio para determinar los requerimientos mínimos del área?

5. ¿Cuenta la empresa con la documentación necesaria del Sistema de Información?

6. ¿El personal que labora en el Área de Consulta Externa está capacitada en el uso del Sistema de Información?

7. ¿Los equipos de Cómputo del Área de Consulta Externa cumple con las especificaciones técnicas necesarias para el buen funcionamiento del Sistema de Información?

8. ¿El Área de Consulta Externa tiene diseñado las políticas en la utilización de los equipos? Cuáles?

9. ¿Cuenta el área con una persona encargada para realizar las copias de seguridad de la información?

10. ¿Cuenta la empresa con un espacio específico para salvaguardar las Copias de Seguridad?

11. ¿Cuáles son los problemas o fallas que se presentan en el módulo de Consulta Externa?

ENCUESTA PARA EL PERSONAL ADMINISTRATIVO

Objetivo: Verificar la veracidad de la información recolectada en la Entrevista.

1. ¿Conoce los lineamientos de la organización en donde se estipulen las líneas de mando definidas por la misma?

   Si____ No____ Por qué?_____

2. ¿De qué forma la empresa da a conocer las funciones que debe desempeñar en su cargo?

   Escrita ___ Verbal ___ Ninguna de las anteriores __

3. ¿Recibe órdenes por parte de más de un funcionario de la empresa?

   Si ( ) No ( )

4. ¿Considera que la infraestructura física de la empresa es la adecuada para realizar las funciones que le fueron asignadas?

   Si ( ) No ( )

5. ¿Considera que la infraestructura tecnológica de la empresa es la adecuada para realizar las funciones que le fueron asignadas?

   Si ( ) No ( )

6. ¿Considera usted que el sistema de información que actualmente posee la empresa es el indicado para la realización de sus labores?

   Si ( ) No ( ) Por qué? _____

7. ¿Considera usted que el sistema de información es íntegro y confiable?

   Si ( ) No ( ) Por qué? _____

Elija la respuesta marcando con una "X"

8. Cómo considera que es el ambiente de trabajo dentro del Área de Consulta Externa para la realización de sus funciones:

Excelente ( ) Bueno ( ) Regular ( ) Malo ( )

9. La capacitación que le ofreció el Área del Consulta Externa en cuanto al manejo del Sistema de Información fue:

   Excelente ( ) Buena ( ) Regular ( ) Malo ( )

10. Cree usted que los mecanismos de seguridad en la información en el Área de Consulta Externa son:

    Adecuados y suficientes ( )
    Adecuados pero insuficientes ( )
    No son los adecuados ( )
    No existen ( )

11. La conexión a Internet que posee el Área de Consulta Externa satisface sus necesidades en cuanto a:

    Tiempos de respuesta ( )
    Seguridad ( )
    Confiabilidad ( )
    Insatisfecho ( )

LISTA DE CHEQUEO – AREA DE CONSULTA EXTERNA

Objetivo: Verificar la veracidad de la Información obtenida en la Entrevista y en la Encuesta

ITEM	SI	NO	OBSERVACIONES
1. ¿Existe un manual de Organización donde se puedan identificar las funciones del personal encargado del Área de Consulta Externa?			
2. ¿Cuenta la IPS con un inventario físico del recurso tecnológico utilizado en el Área de Consulta Externa?			
3. ¿El Sistema de Información cuenta con perfiles de usuario con verificación de acceso?			
3. ¿Existen equipos apropiados para proteger la información y los dispositivos en caso de una variación del voltaje?			
4. ¿Cuenta los Equipos de Cómputo del Área de Consulta Externa con un antivirus?			
5. ¿Existe un manual de usuario del Sistema en caso de pérdida total o parcial de la Información?			
6. ¿Existe un manual de restauración del Sistema en caso de pérdida total o parcial de la Información?			
7. ¿Existe personal de la organización responsable de efectuar y administrar las copias de seguridad??			
8. ¿Existen medios de almacenamiento físico adecuado para salvaguardar la información?			
9. ¿Existe un espacio físico de almacenamiento adecuado para salvaguardar la información?			
10. ¿Cuenta el Área de Consulta Externa con una infraestructura de red?			
11. ¿Cuenta el Área de Consulta Externa con un espacio Físico adecuado para albergar los equipos de red?			
12. ¿El personal que labora en el Área de Consulta Externa recibió inducción en el Manejo del Módulo?			

MATRIZ DE AUTOEVAUACION DE CONTROLES ISO 27001

			RESPUESTA	VALOR
ITEM	DOMINIO			
5	POLITICA DE SEGURIDAD			
5.1	Política de Seguridad de la Información	Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.		
5.1.1	Documento de la política de seguridad de la información	¿Se tiene una Política de seguridad de la información desarrollada y documentada?	NO SABE	0
5.1.2	Revisión de la política de seguridad de la información	El documento de políticas de seguridad de la información se encuentra publicado? Este es revisado por la dirección constantemente?	NO SABE	0
6	ORGANIZACIÓN DE SEGURIDAD			
6.1	Organización de la SI	Se debería establecer una estructura de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.		
6.1.1	Compromiso de la dirección con la seguridad de la información	¿Se evidencia el compromiso demostrado de la dirección frente a la seguridad de la información en la organización?, Con una asignación explícita y el conocimiento de las responsabilidades de la seguridad de la información?	NO CUMPLE	1
6.1.2	Coordinación de la seguridad de la información	¿Ha sido establecido un proceso para coordinar la implementación o puesta en práctica de las medidas de seguridad de la información?	NO CUMPLE	1
6.1.3	Asignación de responsabilidades para la seguridad de la información	¿Las responsabilidades de la realización de los requisitos/requerimientos/responsabilidades de la seguridad de la información se definen claramente? ¿Han sido definidos?	NO CUMPLE	1
6.1.4	Proceso de autorización para los servicios de procesamiento de información	¿Se ha establecido un proceso de autorización de la dirección para nuevos servicios de procesamiento de información? (Punto de vista del negocio y técnico)	NO CUMPLE	1
6.1.5	Acuerdos sobre confidencialidad	¿Se ha definido un procedimiento de identificación y revisión de los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información?	CUMPLE SATISFACTORIAMENTE	3
6.1.6	Contacto con las autoridades / contactos con grupos de interés especial	¿Existe un acuerdo o contactos con personal externo y/o organizaciones que maneje el tema de la seguridad de la información? incluyendo especialistas de la seguridad de la industria y/o de gobierno;	NO CUMPLE	1
6.1.7	Revisión independiente de la seguridad de la información	autoridades de ley; Proveedores de servicio TI; autoridades de telecomunicaciones?	NO CUMPLE	1
6.2	Partes Externas	Mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso terceras partes o que son procesados, comunicados o dirigidos por éstas.		
6.2.1	Identificación de los riesgos relacionados con las partes externas	¿Una revisión independiente de las prácticas de la seguridad de la información se ha conducido para asegurar viabilidad, eficacia, y conformidad con políticas escritas? ¿Esta establecida la revisión a intervalos de tiempo planificados?	NO CUMPLE	1
6.2.2	Riesgos conexiones con terceros	¿Se han analizado los riesgos para la información y los servicios de procesamiento de información en los procesos de negocio que incluyen o involucran a partes externas?	NO CUMPLE	1
6.2.3	Abordaje de la seguridad cuando se trata con los clientes	¿Se han identificado las medidas de seguridad específicas de combatir riesgos de la conexión de los terceros?	NO CUMPLE	1
6.2.4	Abordaje de la seguridad en los acuerdos con terceras partes	¿Se han identificado los requisitos de seguridad antes de dar acceso a los clientes a los activos o la información de la organización?	NO CUMPLE	1
6.3	Partes Externas (outsourcing)	¿Los requisitos de la seguridad se incluyen en contratos formales con terceras partes?	CUMPLE SATISFACTORIAMENTE	3

7	**CONTROL DE ACTIVOS**			
7.1	**Responsabilidad por los activos**	**Lograr y mantener la protección adecuada de los activos de la organización. Todos los activos se deben incluir y deben tener un dueño designado**		
7.1.1	Inventario de activos	¿Los inventarios de activos importantes asociados a cada sistema de información se han creado?	CUMPLE PARCIALMENTE	2
7.1.2	Propiedad de los activos	¿La información y los activos asociados con los servicios de procesamiento de información tienen asignado un propietario parte de la organización?	CUMPLE PARCIALMENTE	2
7.1.3	Uso aceptable de los activos	¿Se han identificado, documentado e implementado reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información?	NO CUMPLE	1
7.2	**Clasificación de la información**	**Asegurar que la información recibe el nivel de protección adecuado**		
7.2.1	Directrices de clasificación	¿Las pautas de la clasificación de seguridad se han establecido para indicar la necesidad , y las prioridades, de la protección de la seguridad?	CUMPLE PARCIALMENTE	2
7.2.2	Etiquetado y manejo de la información	¿Se ha implementado un procedimiento para el etiquetado y manejo de la información?	NO CUMPLE	1
8	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
8.1	**Antes de la Relación Laboral**	**Asegurar que los empleados, contratistas y usuarios por tercera parte entienden sus responsabilidades y son adecuados para los roles para los que se los considera y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.**		
8.1.1	Roles y responsabilidades	¿Las responsabilidades de la seguridad se incluyen en descripciones de las funciones del empleado?	NO CUMPLE	1
8.1.2	Selección	Son las aplicaciones de empleados para un trabajo revisadas de acuerdo al tipo de trabajo (Cargo) a realizar y los niveles de acceso a información sensible acorde con el cargo a cumplir?	NO CUMPLE	1
8.1.3	Términos y Condiciones laborales	¿Los términos y las condiciones del empleo incluyen la responsabilidad del empleado de la seguridad de la información, incluyendo la duración después del empleo y consecuencias de la falta de satisfacer estos términos?	NO CUMPLE	1
8.2	**Durante la Relación Laboral**	**Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respectos a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano**		
8.2.1	Responsabilidad de la dirección	Se evidencia una exigencia de la dirección para que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización?	NO CUMPLE	1
8.2.2	Educación, formación y concientización sobre la SI	Existe un programa de capacitación a empleados, contratistas, etc. de concientización de seguridad, políticas y procedimientos de seguridad , según sea pertinente para sus funciones laborales?	NO CUMPLE	1
8.2.3	Proceso disciplinario	¿Existe definido un proceso disciplinario formal para los empleados que hayan cometido alguna violación de la seguridad?	NO CUMPLE	1
8.3	**Terminación o cambio**	**Asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.**		
8.3.1	Responsabilidades en la terminación	¿Existe un proceso de terminación donde estén claramente definidas las responsabilidades para llevar a cabo la terminación o el cambio de la relación laboral con empleados?	NO CUMPLE	1
8.3.2	Devolución de activos	¿Existe establecido un procedimiento aplicado a los empleados, contratistas u usuarios de terceras partes donde se establezca como parte del mismo la devolución todos los activos de la organización que estén en su poder al finalizar su relación laboral, contrato o acuerdo?	NO CUMPLE	1
8.3.3	Retiro de los derechos de acceso	¿Existe un procedimiento (Documentado) de retiro de acceso a los sistemas de procesamiento de información a empleados, contratistas o terceras partes al finalizar la relación laboral, contrato o acuerdo?	NO CUMPLE	1

9	**SEGURIDAD FISICA DEL ENTORNO**			
9.1	**Areas seguras**	**Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.**		
9.1.1	Perímetro de seguridad física	¿Existen elementos de seguridad física para proteger las áreas que contienen información y servicios de procesamiento?	NO CUMPLE	1
9.1.2	Controles de acceso físico	¿Se emplean los controles de la entrada en áreas seguras para asegurar ingreso solamente a personal autorizado?	NO CUMPLE	1
9.1.3	Seguridad de oficinas, recintos y servicios	¿Es la seguridad física para los centros de datos y las salas de cómputo conmensurada con amenazas? (Documentada)	NO CUMPLE	1
9.1.4	Protección contra amenzas externas y ambientales	¿Existen mecanismos de protección física contra daño por incendio, inundación, terremoto, explosión, malestar social y otras formas de desastre natural o artificial?	NO CUMPLE	1
9.1.5	Trabajo en áreas seguras	¿Se utilizan controles adicionales para el personal o los terceros que trabajan en el área segura?	NO SABE	0
9.1.6	Áreas de carga, despaho y acceso	¿Existen controles en los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones? Estos puntos se encuentran aislados de los servicios de procesamiento de información?	NO SABE	0
9.2	**Seguridad de los equipos**	**Evitar pérdida, daño, robo o puesta en peligro de los activos y la interrupción de las actividades de la organización**		
9.2.1	Ubicación y protección de los equipos	¿El equipo se localiza para reducir riesgos de peligros ambientales y del acceso no autorizado?	CUMPLE PARCIALMENTE	2
9.2.2	Servicios de soporte	¿El equipo electrónico se protege contra apagones y otras anomalías eléctricas?	CUMPLE PARCIALMENTE	2
9.2.3	Seguridad del cableado	¿El cable de la energía y de las telecomunicaciones se protege contra la interceptación o daño?	CUMPLE PARCIALMENTE	2
9.2.4	Mantenimiento de los equipos	¿Se han establecido procedimientos para correcto mantenimiento de equipos y de esta forma asegurar su disponibilidad e integridad de manera continua?	NO SABE	0
9.2.5	Seguridad de los equipos fuera de las instalaciones	¿Se aplica la misma seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización?	NO CUMPLE	1
9.2.6	Seguridad en la reutilización o eliminación de los equipos	¿Existe algún mecanismo para tratamiento de equipos una vez estos se reutilizan o eliminan? (Procedimiento)	NO SABE	0
9.2.7	Retiro de propiedad	¿Existe un procedimiento definido para retiro de equipos, información o software bajo previa autorización de la gerencia?	NO CUMPLE	1
10	**GESTION DE LAS COMUNICACIONES Y OPERACIONES**	**GESTIÓN DE COMUNICACIONES Y OPERACIONES**		
10.1	**Procedimientos de Op. y Resp.**	**Asegurar la operación correcta y segura de los servicios de procesamiento de información.**		
10.1.1	Procedimientos de operación documentados	¿Se documentan los procedimientos de operación (funcionamiento) para que todos los sistemas informáticos aseguren su operación correcta y segura?		#N/A
10.1.2	Gestión del cambio	¿Hay un proceso para el control de los cambios a las instalaciones de IT y los sistemas para asegurar el control satisfactorio de los equipos, software o a los procedimientos?		#N/A
10.1.3	Distribución de funciones	¿Están establecidas separaciones entre las funciones y las áreas de responsabilidad para reducir las oportunidades de la modificación no autorizada o el mal uso de datos o de servicios? Especifique.		#N/A
10.1.4	Separación de las instalaciones de desarrollo, ensayo y op	¿Las instalaciones de desarrollo, ensayo(Prueba) y producción (Operación) se separan para reducir el riesgo de cambios accidentales o del acceso no autorizado al software operacional y a los datos de negocio?		#N/A
10.2	**Gestión servicios de terceros**	**Implementar y mantener un grado adecuado de seguridad de la información y de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceras partes**		
10.2.1	Prestación del servicio	¿Los controles de seguridad, las definiciones del servicio y los niveles de prestación incluidos en el acuerdo de prestación del servicio por terceras partes, están siendo implementados, mantenidos y operados por las terceras partes?		#N/A
10.2.1	Monitoreo y revisión de los servicios por terceras partes	¿Se controlan y revisan los servicios, reportes y registros suministrados por terceras partes?		#N/A
10.2.3	Gestión de los cambios en los servicios por terceras partes	¿Se posee un procedimiento de gestión de cambios en la prestación de servicios con terceras partes? Incluir mantenimiento, mejoras de políticas existentes de seguridad, procedimientos, sistemas, etc.		#N/A
10.3	**Planificación y aceptación del sistema**	**Minimizar el riesgo de fallas en los sistemas**		
10.3.1	Gestión de la capacidad	¿Se supervisan o hacen seguimiento los requisitos de la capacidad, y se proyectan los requisitos futuros, para reducir el riesgo de la sobrecarga del sistema?		#N/A
10.3.2	Aceptación del sistema	¿Los criterios de la aceptación para los nuevos sistemas se han establecido?, y las pruebas convenientes se han realizado antes de la aceptación?		#N/A

10.4	**Protección contra códigos móviles y maliciosos**	**Proteger la integridad del software y de la información**		
10.4.1	Controles contra código maliciosos	¿Se han implementado las medidas preventivas de detección y prevención de virus y los procedimientos del concientización de usuarios?	CUMPLE PARCIALMENTE	2
10.4.2	Controles contra códigos moviles	¿Existe una política de seguridad definida para la autorización y tratamiento de código móvil ?	NO CUMPLE	1
10.5	**Respaldo**	**Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.**		
10.5.1	Respaldo de información	¿Se ha establecido un procedimiento para hacer copias de respaldo de los datos y del software esenciales de negocio para asegurarse de que puede ser recuperado después de un desastre de sistema de cómputo o de una falta de los medios?	CUMPLE PARCIALMENTE	2
10.6	**Gestión de Seguridad de las redes**	**Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.**		
10.6.1	Controles de las redes	¿Existen controles apropiados que aseguran la seguridad de datos en redes, y la protección de servicios conectados contra el acceso no autorizado?	NO CUMPLE	1
10.6.2	Seguridad de los servicios de red	Se tiene claro que en cualquier acuerdo sobre servicios de red se deberían identificar e incluir las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red? ¿Se sigue esta práctica?	NO CUMPLE	1
10.7	**Manejo de los medios**	**Evitar la divulgación, modificación, retiro o destrucción de activos no autorizada y la interrupción en las actividades de negocio**		
10.7.1	Gestión de los medios removibles	¿Existen procedimientos para la gestión de los medios removibles de las computadoras tales como cintas, discos, cassettes, e informes impresos?	NO CUMPLE	1
10.7.2	Eliminación de los medios	¿Existe un proceso implementado para asegurarse que los medios de la computadora son eliminados con seguridad cuando estos no se necesitan más?	NO CUMPLE	1
10.7.3	Procedimientos para el manejo de la información	¿Existen procedimientos para manejar datos sensibles y para proteger tales datos contra acceso no autorizado o divulgación?	NO CUMPLE	1
10.7.4	Seguridad de la documentación del sistema	¿La documentación del sistema se protege contra el acceso no autorizado?	NO CUMPLE	1
10.8.	**Intercambio de Información**	**Mantener la seguridad de la información y del software que se intercambian dentro de la organización y con cualquier entidad externa.**		
10.8.1	Políticas y procedimientos para el intercambio de información	¿Existen establecidas políticas, procedimientos y controles formales de intercambio para proteger el intercambio de información a través del uso de todos los tipos de servicio de comunicación?		#N/A
10.8.2	Acuerdos para el intercambio	¿Existen acuerdos para el intercambio de información y software entre la organización y partes externas?		#N/A
10.8.3	Medios Físicos en Tránsito	¿Se aplican controles para salvaguardar a los medios de la computadora que son transportados entre sitios para reducir al mínimo su vulnerabilidad al acceso no autorizado, al mal uso, o a la corrupción durante el transporte?		#N/A
10.8.4	Mensajería electrónica	¿Se aplican controles cuando sea necesario reducir los riesgos de negocio y de seguridad asociados con el correo electrónico para dar frente a la interceptación, la modificación y errores?		#N/A
10.8.5	Sistemas de información del negocio	¿Existen desarrolladas e implementadas políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio?		#N/A
10.9.	**Servicios de Comercio Electrónico**	**Garantizar la seguridad de los servicios de comercio electrónico y su utilización segura.**		
10.9.1	Comercio Electrónico	¿Se aplican controles de la seguridad para proteger comercio electrónico (los datos electrónicos intercambian, correo electrónico, y las transacciones en línea a través de una red pública tal como el Internet) contra la interceptación o la modificación desautorizada?		#N/A
10.9.2	Transacciones en línea	¿Se implementan mecanismos de protección de información en transacciones en línea para evitar transmisión incompleta, enrutamiento inadecuado, alteración no autorizada del mensaje, divulgación no autorizada, duplicación o repetición no autorizada del mensaje?		#N/A
10.9.3	Información disponible al público	¿Hay un proceso formal de la autorización antes de que la información se haga disponible al público?		#N/A

10.10.	**Monitoreo**	**Detectar actividades de procesamiento de información no autorizada**		
10.10.1	Registro para auditoría	¿Existe procedimiento o disposición para mantener y elaboran durante un periodo acordado la grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.?	NO CUMPLE	1
10.10.2	Monitoreo del uso del sistema	¿Existen procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo y se revisan con regularidad.?	NO CUMPLE	1
10.10.3	Protección de la información del registro	¿Existen controles (Procedimientos) para el manejo y almacenamiento de la información con el fin de protegerla contra divulgación no autorizada o uso inadecuado?		#N/A
10.10.4	Registros de administrador y de operador	¿Se mantiene un registro de las actividades tanto del operador como del administrador del sistema?		#N/A
10.10.5	Registro de fallas	¿Existe cultura o reglas definidas para el registro para posterior análisis sobre fallas? Y basado en estas tomar las acciones adecuadas?		#N/A
10.10.6	Sincronización de relojes	¿Se han fijado a un estándar para asegurar la exactitud de los registros de la auditoria respecto al tiempo, donde se mantengan sincronizados los relojes de los sistemas o dispositivos de comunicaciones?		#N/A
11..	**CONTROL DE ACCESO**	**CONTROL DE ACCESO**		
11.1.	**Requisitos del negocio para el control de acceso**	**Controlar el acceso a la información**		
11.1.1	Política de control del acceso	¿Los requisitos del negocio se definen y se documentan para el control de acceso?	NO CUMPLE	1
11.2.	**Gestión de Acceso de Usuarios**	**Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información**		
11.2.1	Registro de usuarios	¿Hay un procedimiento formal del registro y de la cancelación de registro del usuario para el acceso a todos los servicios de información?	NO CUMPLE	1
11.2.2	Gestión de privilegios	¿Hay restricciones y controles sobre la asignación y uso de privilegios de los usuarios en los sistemas de información (Multiusuario)? ¿Existe un proceso formal para esto?	NO CUMPLE	1
11.2.3	Gestión de contraseñas para usuarios	¿Se ha establecido un proceso formal de gestión de las contraseñas?	NO CUMPLE	1
11.2.4	Revisión de los derechos de acceso de los usuarios	¿Existe un proceso formal para la revisión periódica de los derechos de acceso de usuarios?	NO CUMPLE	1
11.3.	**Responsabilidades de los usuarios**	**Evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información**		
11.3.1	Uso de contraseñas	¿Se han enseñado los usuarios buenas prácticas de la seguridad en la selección y el uso de contraseñas?	NO CUMPLE	1
11.3.2	Equipo de usuario desatendido	¿Se concientiza a todos los usuarios y contratistas de los requisitos y de los procedimientos de la seguridad para proteger equipo desatendido? ¿Están todos los usuarios y contratistas concientizados de sus responsabilidades de poner tal protección en ejecución?	NO CUMPLE	1
11.3.3	Política de escritorio despejado y de Pantalla despejada	¿Se tiene adoptada una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información?	NO CUMPLE	1
11.4.	**Control de Acceso a redes**	**Evitar el acceso no autorizado a servicios en red**		
11.4.1	Política del uso de los servicios en red	¿Un proceso existe para asegurarse de que la red y los servicios informáticos que se pueden alcanzar por un usuario individual o de una Terminal particular son consistentes con la política del control de acceso del negocio?	NO CUMPLE	1
11.4.2	Autenticación de usuarios para conexiones externas	¿Las conexiones de los usuarios remotos vía redes públicas o no pertenecientes a la organización se autentican para prevenir el acceso no autorizado a las aplicaciones del negocio?	NO CUMPLE	1
11.4.3	Identificación de los equipos en las redes	¿Existe un mecanismo de identificación automática de los equipos que sirva para autenticar conexiones de equipos y lugares específicos? ¿Qué métodos se utilizan para dicha identificación?	NO CUMPLE	1
11.4.4	Protección de los puertos de configuración y diagnóstico remoto	¿Existe un proceso para controlar el acceso a los puertos de diagnóstico diseñados para el uso remoto por personal autorizado?	NO CUMPLE	1
11.4.5	Separación en las redes	¿Las redes grandes se han dividido en dominios separados para atenuar el riesgo del acceso no autorizado a los sistemas informáticos existentes que utilizan la red?	NO CUMPLE	1
11.4.6	Control de las conexiones en red	¿Se han incorporado controles para restringir la capacidad de la conexión de usuarios en aquellas redes que se extienden mas allá de las fronteras de la organización? (Dando cumplimiento a la política de acceso y requisitos de aplicación del negocio)	NO CUMPLE	1
11.4.7	Control del enrutamiento en la red	¿Se han incorporado controles de enrutamiento a través de los límites de organización para asegurarse de que las conexiones de los sistemas de cómputo y la información fluye de acuerdo con la política del acceso de las unidades de negocio?	NO CUMPLE	1

11.5.	**Control de Acceso al sistema Operativo**	**Evitar el acceso no autorizado a los sistemas operativos**		
11.5.1	Procedimientos de ingreso seguros	¿Existe un procedimiento de registro de inicio seguro en los sistemas operativos?	NO CUMPLE	1
11.5.2	Identificación y autenticación del usuario	¿Todos los usuarios tienen un identificador único (userID) para su uso personal y único, para asegurarse de que sus actividades se pueden rastrear?	NO CUMPLE	1
11.5.3	Sistema de gestión de contraseñas	¿Un sistema de gestión eficaz de la contraseña se emplea para autenticar a usuarios?	NO CUMPLE	1
11.5.4	Uso de las utilidades del sistema	¿Se restringen los programas utilitarios de sistema que se podrían utilizar para pasar los controles de sistema y aplicaciones? Su uso es restringido?	NO CUMPLE	1
11.5.5	Tiempo de inactividad de la sesión	¿Las terminales en localizaciones de riesgo elevado se les configurada bloqueo cuando son inactivos por cierto tiempo a fin de prevenir el acceso por personas no autorizadas?	NO CUMPLE	1
11.5.6	Limitación del tiempo de conexión	¿Se ha fijado un límite en el período durante el cual los terminales se pueden conectar con los sistemas de uso sensibles?	NO CUMPLE	1
11.6.	**Control de Acceso a las Aplicaciones y a la Información**	**Evitar el acceso no autorizado a la información contenida en los sistemas de información**		
11.6.1	Restricción del acceso a la información	¿El acceso a los datos y a las funciones del sistema de aplicaciones se restringe de acuerdo con la política de acceso definida y esta se basa en requisitos individuales?	NO CUMPLE	1
11.6.2	Aislamiento de sistemas sensibles	¿Según riesgos identificados, los sistemas de aplicaciones sensibles funcionan en un ambiente de proceso aislado?	NO CUMPLE	1
11.7.	**Computación Móvil y Trabajo Remoto**	**Garantizar la seguridad de la información cuando se utilizan dispositivos de computación móviles y de trabajo remoto**		
11.7.1	Computación y comunicaciones móviles	¿Se ha desarrollado una política formal que trata los riesgos del trabajo con las instalaciones de computación móvil, que incluyan los requisitos para la protección física, los controles de acceso, las técnicas criptográficas, el respaldo, y la protección de virus?	NO CUMPLE	1
11.7.2	Trabajo remoto	¿Las políticas y los procedimientos se han desarrollado para controlar teleworking, las instalaciones existentes que abarcaban, el ambiente teleworking propuesto, requisitos de la seguridad de comunicaciones, y la amenaza del acceso no autorizado al equipo o a la red?	NO CUMPLE	1
12..	**ADQUISICIÓN, DESARROLLO y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**	**ADQUISICIÓN, DESARROLLO y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN**		
12.1.	**Requisitos de seguridad de los sistemas de información**	**Garantizar que la seguridad es parte integral de los sistemas de información**		
12.1.1	Análisis y especificación de los requisitos de seguridad	¿Se realiza un análisis de los requisitos de la seguridad como parte de la etapa del análisis de requisitos de cada proyecto del desarrollo?		#N/A
12.2.	**Procesamiento correcto de las aplicaciones**	**Evitar errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones**		
12.2.1	Validación de los datos de entrada	¿Los Datos que se ingresan en sistemas de aplicaciones se validan para asegurarse de que son correctos y apropiados?		#N/A
12.2.2	Control del procesamiento interno	¿Chequeos de validación se han incorporado en sistemas para detectar la corrupción causada por errores de proceso o por actos deliberados?		#N/A
12.2.3	Integridad del mensaje	¿La autentificación del mensaje se ha considerado para las aplicaciones que implican la transmisión de datos sensibles?		#N/A
12.2.4	Validación de los datos de salida	¿Los datos de salida de los sistemas de aplicación se validan para asegurarse de que son correctos y apropiados?		#N/A
12.3.	**Controles Criptográficos**	**Proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos**		
12.3.1	Política sobre el uso de controles criptográficos	¿La gerencia ha desarrollado una política en el uso de controles criptográficos, incluyendo la gerencia de las llaves del cifrado, y se implementación eficaz?		#N/A
12.3.2	Gestión de llaves	¿Es un sistema de administración implementado para soportar el uso en la organización de lleves publicas y llevas privadas?		#N/A
12.4.	**Seguridad de los archivos del sistema**	**Garantizar la seguridad de los archivos del sistema**		
12.4.1	Control del software operativo	¿Se tiene un estricto control sobre la implementación de software en sistemas operacionales?		#N/A
12.4.2	Protección de los datos de prueba del sistema	¿Se protegen y se controlan todos los datos de la prueba de los sistemas de aplicación?		#N/A
12.4.3	Control del acceso al código fuente de programas	¿Para reducir el potencial para la corrupción de los programas de computadora, el acceso a las bibliotecas fuente del programa es estrictamente controlado?		#N/A

12.5.	**Seguridad en los procesos de desarrollo y soporte**	**Mantener la seguridad del software y de la información del sistema de aplicaciones**		
12.5.1	Procedimientos de control de cambios	¿Se ha implementado un procedimiento formal de control de cambios?		#N/A
12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	¿Se revisan los sistemas de aplicaciones cuando ocurren cambios a nivel de los sistemas operativos?		#N/A
12.5.3	Restricciones en los cambios a los paquetes de software	¿Se desalienta la realización de modificaciones a los paquetes de software? ¿Se limitan a los cambios necesarios, y todos los cambios se controlan estrictamente?		#N/A
		¿Se consideran los siguientes aspectos para limitar el riesgo de fuga de información, por ejemplo, mediante el uso y explotación de los canales encubiertos?		#N/A
		a) exploración de los medios y comunicaciones de salida para determinar la información oculta;		#N/A
		b) comportamiento de las comunicaciones y del sistema de modulación y enmascaramiento para reducir la probabilidad de que una tercera parte pueda deducir información a partir de tal comportamiento;		#N/A
		c) utilización de sistemas y software que se consideran con integridad alta, por ejemplo usar productos evaluados (véase la norma ISO/IEC 15408);		#N/A
		d) monitoreo regular de las actividades del personal y del sistema, cuando está permitido por la legislación o los reglamentos existentes;		#N/A
12.5.4	Fuga de Información (Canales Encubiertos y Código Troyano)	e) monitoreo del uso de los recursos en los sistemas de computador		#N/A
12.5.5	Desarrollo de software contratado externamente	¿Cuando desarrollo del software es por outsourcing, se definen los detalles para proteger, supervisar y monitorear el desarrollo?		#N/A
12.6.	**Gestion de las Vulnerabilidades**	**Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.**		
12.6.1	Control de las vulnerabilidades técnicas	¿Se obtiene información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso? ¿Se evaluar la exposición de la organización a dichas vulnerabilidades y se toman las acciones apropiadas para tratar los riesgos asociados?		#N/A
13..	**GESTIÓN DE INCIDENTES - MONITOREO**			
13.1.	**Reporte sobre los eventos y las debilidades de seguridad de la información**	**Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente**		
13.1.1	Reporte sobre los eventos de seguridad de la información	¿Existen procedimientos formales de reportes y respuesta a incidentes para identificar las acciones a ser tomadas frente a la recepción de un reporte de incidentes?		#N/A
13.1.2	Reporte sobre las debilidades en la seguridad	¿Son los usuarios requeridos observar y reportar todas las debilidades de seguridad observadas o sospechadas o amenazas a los sistemas o a los servicios?		#N/A
13.2.	**Gestión de los incidentes y las mejoras en la seguridad de la información**	**Asegurar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.**		
13.2.1	Responsabilidades y procedimientos	¿Se ha establecido las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información?		#N/A
13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	Existen implementados mecanismos para monitorear los tipos, los volúmenes, y los costos de incidentes y de malfuncionamientos?		#N/A
13.2.3	Recolección de evidencias	¿Existen definidos procedimientos para que se debería recolectar, retener y presentar evidencia para cumplir las reglas de la evidencia establecidas en la jurisdicción pertinente?		#N/A
14..	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
14.1.	**Aspectos de seguridad de la información en la Gestión de la Continuidad de Negocios**	**Contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y asegurar su recuperación oportuna.**		
14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio	¿Se ha desarrollado y mantenido un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización?		#N/A
14.1.2	Continuidad del negocio y evaluación de riesgos	¿Se han identificado los eventos que pueden ocasionar interrupciones en los procesos del negocio junto con la probabilidad y el impacto de dichas interrupciones, así como sus consecuencias para la seguridad de la información?		#N/A
14.1.3	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información	¿En el proceso del planeamiento de la continuidad del negocio ha incluido la identificación y el acuerdo de todas las responsabilidades y procedimientos de emergencia?		#N/A
14.1.4	Estructura para la planificación de la continuidad del negocio	¿Se mantiene un único marco (framework) del plan de la continuidad del negocio para asegurarse de que todos los niveles del plan son consistentes?		#N/A
14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	¿Los planes de la continuidad del negocio se prueban regularmente para asegurarse de que son actuales y eficaces?		#N/A

15..	**CUMPLIMIENTO**	**CUMPLIMIENTO**		
15.1.	**Cumplimiento de los requisitos legales**	**Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales y de cualquier requisito de seguridad**		
15.1.1	Identificación de la legislación aplicable	¿Todos los requisitos estatutarios, reguladores, y contractuales relevantes son específicamente definidos y se documentan para cada sistema de información?	NO CUMPLE	1
15.1.2	Derechos de propiedad intelectual (DPI)	¿Hay conformidad con restricciones legales en el uso de material con copyright asegurándose que solamente el software se desarrolló en la organización, o licenciado o proporcionado por el desarrollador a la organización, es utilizado?	NO CUMPLE	1
15.1.3	Protección de los registros de la organización	¿Los registros de la organización importantes se mantienen con seguridad para dar cumplimiento a requisitos estatutarios, así como para apoyar actividades económicas esenciales?	NO CUMPLE	1
15.1.4	Protección de los datos y privacidad de la información personal	¿Las aplicaciones que procesan datos personales dan cumplimiento a la legislación aplicable de la protección de los datos?	NO CUMPLE	1
15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	¿Las instalaciones de IT se utilizan solamente para los propósitos del negocio?	NO CUMPLE	1
15.1.6	Reglamentación de los controles criptográficos	¿El asesoramiento jurídico se ha buscado en la conformidad de la organización con leyes nacionales e internacionales sobre controles criptográficos?	NO CUMPLE	1
15.2.	**Cumplimiento de las Políticas y las normas de seguridad y cumplimiento técnico**	**Asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización**		
15.2.1	Cumplimiento con las políticas y las normas de seguridad	¿Todas las áreas dentro de la organización son consideradas para revisiones con regularidad que asegure conformidad con políticas y estándares de la seguridad?	NO CUMPLE	1
15.2.2	Verificación del cumplimiento técnico	¿Las instalaciones de IT se comprueban regularmente para saber si hay conformidad con los estándares seguridad implementados?	NO CUMPLE	1
15.3.	**Consideraciones de la Auditoría de los sistemas de Información**	**Maximizar la eficacia de los procesos de auditoría de los sistemas de información y maximizar su interferencia**		
15.3.1	Controles de auditoría de los sistemas de información	¿Las auditorias y las actividades que implican chequeos en sistemas operacionales se planean y se arreglan cuidadosamente?	NO CUMPLE	1
15.3.2	Protección de las herramientas de auditoría de los sistemas de información	¿El acceso a las herramientas de auditoria del sistema es controlado?	NO CUMPLE	1
				#N/A
		GRADO O NIVEL DE CUMPLIMIENTO NORMA ISO27001	CUMPLE PARCIALMENTE	**22%**