

UNIVERSIDAD NACIONAL DE INGENIERIA

Facultad de Ingeniería Industrial y de Sistemas



**IMPLEMENTACIÓN DEL SISTEMA DE PROTECCIÓN DE LA
INFORMACIÓN EMPRESARIAL EN UNA EMPRESA DE
TELECOMUNICACIONES**

**INFORME DE SUFICIENCIA
Para optar el Título Profesional de**

INGENIERO DE SISTEMAS

CHRISTIAN LUIS MEZA VILLAFUERTE

**LIMA - PERU
2007**

DEDICATORIA

Dedicado a mis padres Lucho y Betty, quienes siempre supieron inculcarme una buena educación y brindarme valores necesarios para mi formación.

Cada uno de los integrantes de mi familia tiene un espacio en mi mente y en mi corazón, especialmente a mi linda abuelita Victoria, quien desde el cielo ilumina mi vida y me guía en el camino del bien.

A todas aquellas amistades que cooperaron siempre conmigo, mi eterna gratitud. Igualmente para mis compañeros de trabajo.

SISTEMA DE PROTECCIÓN DE LA INFORMACIÓN EMPRESARIAL EN UNA EMPRESA DE TELECOMUNICACIONES

ÍNDICE	3
DESCRIPTORES TEMÁTICOS	7
RESUMEN EJECUTIVO	8
INTRODUCCIÓN	10

CAPÍTULO 1. ANTECEDENTES

1.1 Diagnóstico del Sector de Telecomunicaciones	12
1.1.1 Características Generales	14
1.1.2 Marco Legal	15
1.1.3 Evolución	16
1.1.4 Cadena de Valor del Sector	18
1.2 Diagnóstico Estratégico	22
1.2.1 Descripción del Grupo	22
1.2.2 Misión	24
1.2.3 Visión	

1.2.4 Valores Corporativos	25
1.2.5 Información Financiera	26
1.2.6 Análisis Externo	28
1.2.7 Análisis Interno	30
1.2.8 Análisis FODA	33
1.2.9 Área de la Organización en Estudio	34
1.3 Diagnóstico Funcional	40
1.3.1 Productos y Servicios	40
1.3.2 Clientes	41
1.3.3 Proveedores	41
1.3.4 Empresas del Grupo	42

CAPÍTULO 2. MARCO TEÓRICO

2.1 Seguridad de la Información	45
2.1.1 Conceptos Generales	45
2.1.2 Seguridad de la Información	47
2.1.3 Políticas de Seguridad	49
2.1.4 Información Confidencial	54
2.1.5 Otros medios de protección interna de la información confidencial	55
2.1.6 Protección de la Información compartida con Outsourcing	
2.2 Metodología de Desarrollo MEGON	57

2.2.1 Modelo de Gestión MEGON	57
2.2.2 Estructura del MEGON	60
2.2.3 Hitos y Entregables	61

CAPÍTULO 3: PROCESO DE TOMA DE DECISIONES

3.1 Planteamiento del Problema	66
3.2 Alternativas de Solución	67
3.3 Metodología de Solución	69
3.4 Toma de Decisiones	74
3.5 Estrategias Adoptadas o Implementación	75
3.5.1 Cronograma del Proyecto	75
3.5.2 Descripción General del Sistema	77
3.5.3 Objetivos del Sistema	77
3.5.4 Alcance del Sistema	78
3.5.5 EDT del Proyecto	79
3.5.6 Descripción de Entregables del Proyecto	80
3.5.7 Costo del Proyecto	81
3.5.8 Fase de Análisis y Modelamiento	82
3.5.8.1 Módulos del Sistema	82
3.5.8.2 Diagramas de Casos de Uso	83
3.5.8.3 Diagramas de Clases	84
3.5.8.3 Diagramas de Actividades	86

3.5.9 Fase de Diseño	90
3.5.9.1 Prototipos del Sistema	90
3.5.9.2 Diseño Externo del Sistema	99
3.5.10 Diseño de Archivos Físicos	99
3.5.10.1 Diagrama de Base de Datos	103
3.5.10.2 Modelo de Datos	104
3.5.11 Fase de Pruebas	110
3.5.12 Fase de Implementación	111
3.5.12.1 Centros de Impleemntación	111
3.5.12.2 Arquitectura del Sistema	112
3.5.12.3 Estrategia de Implementación	114
3.5.12.4 Planificación	114
CAPÍTULO 4: EVALUACIÓN DE RESULTADOS	115
CONCLUSIONES Y RECOMENDACIONES	117
GLOSARIO DE TÉRMINOS	119
BIBLIOGRAFÍA	120
ANEXOS	121

DESCRIPTORES TEMÁTICOS

- Protección de la Información Empresarial
- Seguridad Informática
- Base de Datos Documentales
- Telecomunicaciones
- Incidencias TI

RESUMEN EJECUTIVO

Uno de los activos valiosos de cualquier organización es la información, y si hablamos de la información empresarial pues con mayor razón. Es por ello que se establecen políticas y normativas para controlar la seguridad y la protección de la información empresarial. Estas políticas se incluyen en la normativa general de Seguridad de la Información.

Actualmente se maneja en la organización a la cual analizo, manualmente, la identificación de los trabajadores con riesgos o incidencias de la Protección de la Información Empresarial (PIE), incluso cada área utiliza diversos formatos o plantillas, resultando dificultosa la emisión de reportes mensuales a la gerencia. Además, existe tanta información en las oficinas remotas que en los centros de datos, incluso pudiendo ser objeto de manipulaciones por parte del personal.

Para solucionar dicho problema, se propuso desarrollar un sistema que permita automatizar dicha identificación, centralizando la información, además que permita tener mayor exactitud y frecuencia en la identificación de los riesgos de protección de la información en todos los locales de los clientes del servicio PIE.

El desarrollo del aplicativo se basó en la metodología MEGON, utilizado para el desarrollo de cualquier software del Grupo, produciendo diversos entregables que abarcan desde la concepción del sistema hasta su implantación final y el acta de aceptación del cliente.

El presente informe explica cómo se propuso el aplicativo, las características técnicas del mismo, la arquitectura requerida, el plan de pruebas, y al final los resultados obtenidos. Cabe destacar que el cliente requiere contar únicamente con un navegador web para tener acceso al sistema, a través de Internet.

Queda a vuestra disposición el presente trabajo.

INTRODUCCIÓN

El presente trabajo monográfico trata acerca del desarrollo del proyecto de un sistema que permite automatizar las incidencias ocurridas referentes a la Protección de la Información Empresarial (PIE) de la organización.

La solución automatiza el proceso de registro de las incidencias ocurridas, para ello los vigilantes y personal autorizado deben estar capacitados para manejar y aprovechar al máximo el software desarrollado, en aras de una buena gestión contra dichas incidencias.

Este aplicativo resuelve un problema de seguridad, pues el formato actual es susceptible de cambio por ser un documento Excel (manipulación del archivo por parte del trabajador). El aplicativo al manejar el registro de incidencias mediante Lotus Notes permita desterrar esa posibilidad, siendo la información fiable y centralizada.

Asimismo es necesario señalar que la solución propuesta depende estrictamente de una conexión a Internet, el aplicativo para ser utilizado se necesita tener instalado Lotus Notes. El sistema tiene un rendimiento óptimo, razón por la cual no es necesario disponer de una PC muy equipada o con mucha memoria.

El proyecto tuvo acogida en la empresa, el proveedor fue seleccionado frente a 2 competidores, de acuerdo a criterios económicos, tecnológicos y de satisfacción. En el presente trabajo se explican los criterios que llevaron a elegir la solución propuesta por el proveedor seleccionado.

Se incluye también en el presente informe la arquitectura del sistema, los costos incurridos, beneficios de la solución, pantallas del sistema, los módulos generados y los reportes posibles de generar.

CAPÍTULO 1

ANTECEDENTES

1.1 DIAGNÓSTICO DEL SECTOR DE TELECOMUNICACIONES

En los comienzos de la década de los 90, la situación de las telecomunicaciones en el Perú era muy precaria. Para disponer de una línea telefónica, había que realizar un trámite que podía demorar hasta años. Sin embargo, esta cambió desde la privatización de la Compañía Peruana de Teléfonos (CPT) y la Empresa Nacional de Telecomunicaciones (Entel) y su adquisición en 1994 por el Grupo. Desde el 1 de agosto de 1998, los mercados de telefonía fija local y de larga distancia nacional e internacional quedaron abiertos al ingreso de nuevos operadores.

En ese año, el sector peruano de telecomunicaciones había expandido sus redes en aproximadamente 167% en comparación con 1993 y la densidad telefónica (es decir, el número de teléfonos por cada 100 habitantes) se había incrementado de 2,9 a comienzos de los años ochenta a 7,8 en 1998.

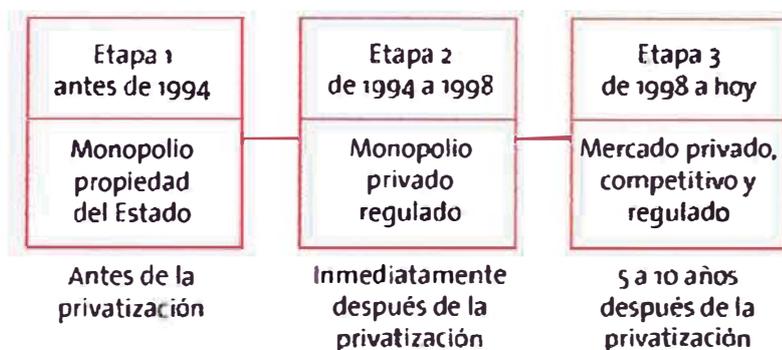


Gráfico N° 1: Las 3 etapas en la reforma de Telecomunicaciones

En los últimos cinco años, el sector telecomunicaciones ha sido el de mayor crecimiento. Su contribución al Producto Bruto se ha duplicado y las inversiones han superado los US\$ 2,500 millones de dólares. En consecuencia, las empresas y los hogares cuentan con una mayor variedad de servicios de mejor calidad a precios que irán reduciéndose progresivamente gracias a la competencia.

El crecimiento registrado refleja diferencias regionales; por ejemplo, del total de líneas telefónicas a nivel nacional, el 66% se encontraban en Lima y Callao, seguidas de Arequipa (6%), La Libertad (4%), Lambayeque y Piura (3% cada una). En los departamentos más pobres, como Huancavelica o Ayacucho, el porcentaje de líneas con respecto al total nacional es 0,1%.

1.1.1 CARACTERÍSTICAS GENERALES

El sector de las telecomunicaciones tiene especial trascendencia para el desarrollo económico ya que éste se sustenta cada vez con más fuerza en la capacidad de establecer un flujo de información que garantice el funcionamiento de mercados eficientes e integrados. Las telecomunicaciones facilitan el acceso al mercado, mejoran los servicios a los clientes, reducen los costos e incrementan la productividad. Asimismo, la inversión en este sector es considerada estratégica para mantener y desarrollar las ventajas competitivas a nivel empresarial, nacional e internacional.

En el Perú, las telecomunicaciones se encuentran inmersas en un proceso de rápido crecimiento, tanto por la ampliación de la cobertura de los servicios tradicionales como por la aparición de otros nuevos.

Las principales actividades del sector son telefonía básica (líneas telefónicas comunes de uso privado), que, junto con la telefonía pública, conforman la telefonía fija. Las líneas en servicio de telefonía fija a nivel nacional se han incrementado de 660 mil en 1993 a 1,85 millones en 1998, es decir, un crecimiento acumulado de 80%. En 1998 el incremento fue 15%. Otra actividad es la telefonía móvil, basada en los teléfonos celulares, cuyas líneas en servicio han tenido un crecimiento acumulado de 1000% entre 1993 y 1998. En el

mercado de la televisión por cable -el servicio de dar acceso a canales de televisión internacionales- las empresas más importantes en el mercado son Cable Mágico, Telecable y Direct TV. Este servicio se ha difundido mucho en los últimos años, alcanzando un total de 250 000 usuarios.

1.1.2 MARCO LEGAL

El marco regulativo que posibilita el desarrollo y la modernización de las redes y servicios de telecomunicaciones en el Perú ha atravesado dos etapas claramente diferenciadas: el de las reformas iniciales y el del adelanto de la apertura de los mercados. La primera, que coincidía con la privatización y un período de concurrencia limitada, tuvo el propósito de lograr una expansión y modernización mínima de la red, en tanto se sinceraban las tarifas en relación con sus costos. La segunda etapa consiste en el desarrollo del sector en plena competencia.

Las telecomunicaciones en el Perú se rigen por la Ley de Telecomunicaciones y su reglamento. Este marco legal busca crear condiciones para atraer la inversión privada requerida para ofrecer servicios modernos cuya calidad, cobertura y diversidad contribuyan al desarrollo nacional bajo una estructura tarifaria competitiva.

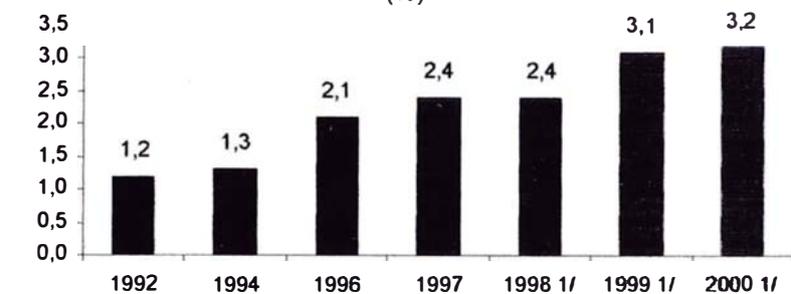
Por otro lado, la labor de regulación por parte del estado ha sido asignada al Organismo para la Supervisión de Inversión Privada en Telecomunicaciones (Osiptel), y se ha creado el Fondo de Inversión de Telecomunicaciones (FITEL), cuya finalidad es financiar los servicios de telecomunicaciones en áreas rurales o en zonas consideradas de interés social prioritario.

Por otro lado, el actual marco legal ha introducido la noción de protección de derechos de los usuarios al establecer que todo concesionario de servicios públicos de telecomunicaciones debe tener procedimientos expeditivos y eficaces sustentados en los principios de transparencia, responsabilidad, equidad y no discriminación para solucionar los reclamos relativos a los servicios que prestan.

1.1.3 PARTICIPACIÓN DEL SECTOR TELECOMUNICACIONES EN EL PBI

Desde la privatización en 1994, las telecomunicaciones han crecido, en promedio, 21,6% por año. Además, el sector ha concentrado el mayor stock de inversión extranjera en los últimos cinco años (33% del total). Sólo el Grupo ha invertido alrededor de US\$ 2 500 millones: US\$ 1 500 millones en la Red Telefónica Básica, US\$ 300 millones en LDN y LDI, US\$ 500 millones en Telefonía Móvil y US\$ 200 millones en TV por Cable.

**PARTICIPACION DEL SECTOR DE
TELECOMUNICACIONES EN EL PBI**
(%)



1/ Estimado

Fuente: Osiptel

Gráfico N° 2: Participación del Sector de Telecomunicaciones en el PBI

Por otro lado, el número de usuarios de los distintos servicios de telecomunicaciones se ha incrementado significativamente. Se han instalado un millón doscientas mil nuevas líneas en telefonía fija entre diciembre de 1993 y junio de 1998, mientras que la densidad telefónica ha aumentado en más del doble. El mercado de teléfonos celulares ha crecido 15 veces entre 1994 y 1998.

**NUMERO DE USUARIOS
DE SERVICIOS DE TELECOMUNICACIONES**

	1994	1997	1998
Telefonía fija	663 000	1 500 000	1 850 000
Celulares	49 000	280 000	720 000
Buscapersonas	35 000	70 000	75 000
Trunking	1 200	20 000	20 000
TV Cable	20 000	250 000	350 000
Acceso a Internet	500	60 000	120 000

Fuente: Osiptel

Gráfico N° 3: Número de Usuarios de Servicios de Telecomunicaciones

Los beneficios de este crecimiento han alcanzado a todos los sectores socioeconómicos. En Lima Metropolitana, la mitad de los hogares cuenta hoy con teléfono. En el nivel socioeconómico D, el porcentaje de hogares con teléfono se ha multiplicado por 20 en los últimos cinco años.

1.1.4 CADENA DE VALOR DEL SECTOR DE TELECOMUNICACIONES

Los agentes fundamentales de la cadena de valor del sector de telecomunicaciones son:

1. Desarrolladores de contenidos y aplicaciones
2. Fabricantes e integradores de equipos y dispositivos
3. Operadores de redes
4. Proveedores de servicios
5. Distribuidores
6. Usuarios

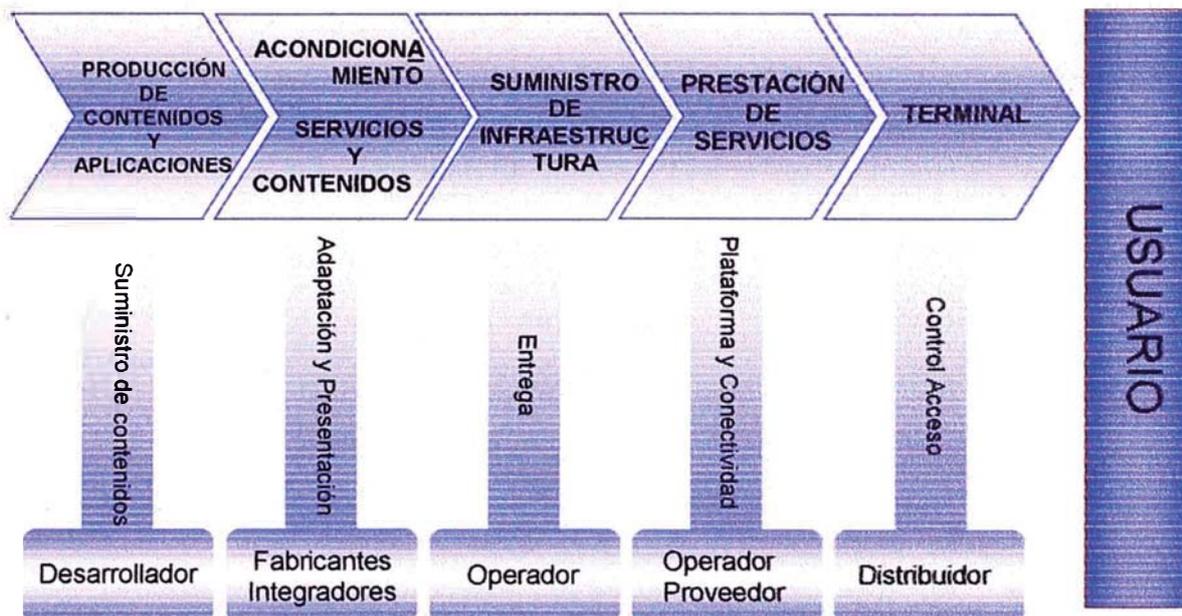


Gráfico N° 4: Cadena de Valor del Sector de Telecomunicaciones

La convergencia permite a los actores del sector de las telecomunicaciones ya existentes desempeñar funciones nuevas. Igualmente, las empresas suelen estar presentes en uno o más elementos de la cadena del valor.

En la siguiente tabla se muestra una breve descripción de cada uno de los agentes:

AGENTE	ROL DEL AGENTE EN LA CADENA DE VALOR
<p>Desarrollador de Contenidos y Aplicaciones</p>	<p>Son los encargados de crear y adaptar los contenidos (producción de videos, generación de imágenes, gestión de la información, etc.) a formatos compatibles para las aplicaciones de acuerdo a los requerimientos de los dispositivos terminales del usuario.</p> <p>También desarrollan aplicaciones que proporcionan la interfase entre el dispositivo y el hardware de la red, brindándoles eficiencia y permitiendo la prestación de nuevos servicios.</p>
<p>Fabricantes de equipos y dispositivos</p>	<p>Aunque tradicionalmente se definen en un solo agente, se pueden distinguir dos roles entre los fabricantes:</p> <ul style="list-style-type: none"> - Fabricantes de equipos: quienes diseñan, fabrican y ensamblan conmutadores, módems e interfaces necesarias entre la red de comunicaciones. - Fabricantes de dispositivos: fabrican los dispositivos terminales que permiten la comunicación de la información (voz, datos, video).

<p>Operadores de Redes</p>	<p>Opera y mantiene la infraestructura (red) que permite la transmisión de la información y los contenidos.</p> <p>El operador de la red compite por la adopción, retención y lealtad del cliente.</p>
<p>Proveedor de Servicios</p>	<p>Tradicionalmente, la prestación de servicios estaba íntimamente ligada a la existencia de una determinada infraestructura. De esta forma eran dos conceptos inseparables: la red que daba soporte físico y el servicio de telecomunicaciones, ambos prestados por un mismo operador.</p> <p>Actualmente, los usuarios pueden disfrutar de una serie de servicios accediendo a sus proveedores con independencia de su operador de red de acceso.</p>
<p>Distribuidor</p>	<p>Es el encargado de la venta de los terminales. Muchas veces este rol es asumido por los proveedores de servicios o por los mismos fabricantes de dispositivos</p>
<p>Usuario Final</p>	<p>Son los consumidores, empresas u otros individuos que acceden a los productos y servicios.</p>

1.2 DIAGNÓSTICO ESTRATÉGICO

1.2.1 DESCRIPCIÓN DE GRUPO

El Grupo es uno de los grandes líderes de telecomunicaciones a nivel mundial, presente en Europa, África y Latinoamérica, mayor cuota de negocio fuera de su mercado de origen y el operador de referencia en el mercado de habla hispano-portuguesa. En septiembre de 2005, el número de clientes del Grupo era de 147,7 millones.

El Grupo está presente en Latinoamérica desde hace 15 años, con una inversión acumulada en infraestructuras y adquisiciones que supera los 70.000 millones de euros, con más de 21,7 millones de accesos fijos, casi 6 millones de accesos de datos e internet y más de 63 millones de accesos de telefonía móvil.

Actualmente es el operador líder en Brasil, Argentina, Chile y Perú y está desarrollando importantes operaciones en Colombia, Ecuador, El Salvador, Guatemala, México, Marruecos, Nicaragua, Panamá, Puerto Rico, Uruguay y Venezuela.

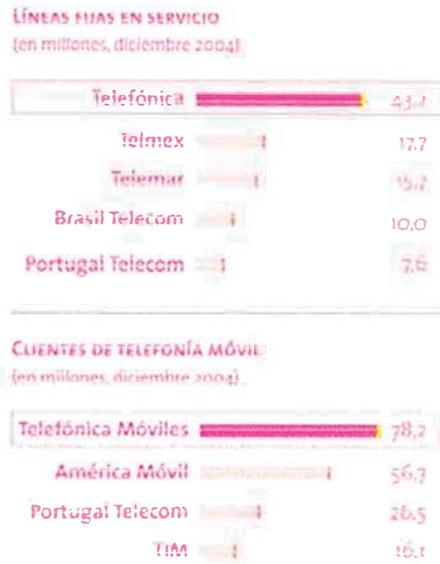


Gráfico N° 5: Ranking de empresas de telecomunicaciones en el mercado de habla hispano portuguesa

La organización por líneas de negocio en el Grupo se muestra en la siguiente figura:



Gráfico N° 6: Organización por Líneas de Negocio del Grupo

1.2.2 MISIÓN

El propósito del Grupo es el de ser reconocidos como un grupo integrado que ofrece soluciones integradas a cada segmento de clientes, tanto de comunicaciones, móviles como fijas, de voz, de datos y de servicios; que está comprometido con sus grupos de interés por su capacidad de cumplir con los compromisos adquiridos con todos: clientes, empleados, accionistas y la sociedad de los países en los que opera.

1.2.3 VISIÓN

El Grupo aspira a convertirse en el mejor y mayor grupo integrado de telecomunicaciones del mundo. El mejor, en orientación al cliente, innovación, excelencia operativa y liderazgo, y compromiso de sus empleados. Y el mayor, tanto en crecimiento y rentabilidad para sus accionistas como en valor de mercado entre las operadoras integradas.

Esta visión se basa en 5 pilares fundamentales: orientación al cliente, innovación, excelencia operativa, liderazgo y compromiso con las personas, e identidad corporativa y comunicación. En el Anexo 1 se encuentra un mayor detalle de estos 5 pilares.

1.2.4 VALORES CORPORATIVOS

El Grupo comparte una misma visión de liderazgo, una misión y unos valores que son el eje de su cultura corporativa. Una cultura sólida y a la vez flexible que le permite adaptarse a los nuevos contextos y a los retos del futuro. Este es el proyecto empresarial del grupo para los próximos años, una meta para todos los que componen esta compañía.

Los valores son la base de la empresa, pues establecen la dirección sobre el cual se va dotando de contenido específico los compromisos que el Grupo adquiere con sus grupos de interés para ganarse su confianza. Así para los accionistas la confianza se traduce en rentabilidad y transparencia; para los clientes, en calidad y cumplimiento; para los empleados, en claridad en la relación y desarrollo profesional; y para la sociedad, en proximidad y contribución.



Gráfico N° 7: Valores Corporativos del Grupo

1.2.5 INFORMACIÓN FINANCIERA

En el primer trimestre de 2006, el Grupo ha mejorado los resultados respecto al mismo trimestre del año anterior, se muestra los resultados obtenidos en el mes de marzo de 2006:



Millones €	1997	1998	1999	2000	2001	2002	2003	2004	2005
Ingresos	14.202,5	17.465,5	22.957,0	28.464,9	31.052,6	28.411,3	28.399,8	30.321,9	37.882,1
EBITDA	7.591,4	9.259,9	10.885,4	11.918,2	12.804,3	11.724,2	12.602,1	13.215,4	
OIBDA								12.222	15.376,4
Beneficio Neto	1.142,3	1.307,7	1.604,7	2.504,7	2.106,8	5.576,6	2.203,6	2.877,3	4.445,8
Deuda Neta	13.926,6	19.211,0	20.824,4	26.950,9	28.941,6	22.533,1	19.235,3	20.962,7	30.067

Gráfico N° 8: Información Financiera

La empresa a nivel local informó que anotó entre enero y marzo ingresos netos por 1.123,1 millones de soles, un 6,5 por ciento más que las ventas de 1.054,9 millones de soles del mismo lapso del 2005.

La empresa reportó el año pasado ganancias por 253,3 millones de soles, un salto frente a los 53 millones de soles del 2004.

1.2.6 ANÁLISIS EXTERNO

El objetivo del análisis del entorno de la empresa es la identificación del escenario más probable en cuanto a las variables externas que afectan en forma directa el accionar de la empresa.

Una **oportunidad** se define como un factor externo a la empresa, pero que es favorable a ella porque facilita y/o ayuda a alcanzar la misión propuesta.

Por el contrario una **amenaza** es un factor externo a la empresa que es desfavorable a ella, porque limita u obstaculiza el alcanzar la misión.

Ámbito Político

- **Posible Cambio de Sistema Económico del País (Amenaza):** Con el nuevo gobierno a asumir la jefatura del Estado, es probable que la política económica cambie a una de tendencia socialista e intervencionista del Estado, que atente contra las inversiones privadas.
- **Leyes de Regulación de Osiptel (Amenaza):** Las recientes normas reguladoras de Osiptel, como la reciente fijación de tarifas sociales, son una amenaza para las utilidades de la empresa.

Ámbito Sociocultural

- **Demografía del País (Oportunidad):** El crecimiento exponencial de la población y la mejora en el nivel de vida de los ciudadanos permitirá una mayor cartera de clientes a captar.
- **Manifestaciones Públicas (Amenaza):** Las continuas manifestaciones públicas en nuestro país contra la empresa atentan contra el prestigio y las utilidades de la misma.

Ámbito Económico Financiero

- **Alta Rentabilidad (Oportunidad):** El sostenido crecimiento del sector permite tener expectativas de utilidades elevadas.
- **Recesión en Perú (Amenaza):** A pesar de lo especificado en el ítem anterior, la recesión sigue siendo un problema existente, sin visos de mejoría en un mediano plazo.

Ámbito Tecnológico

- **Crecimiento del Uso de Internet (Oportunidad):** Cada vez más personas están accediendo a Internet, a tarifas más económicas, con menos burocracia y con mayor dosificación a nivel del país.
- **Masificación del Uso de Celulares (Oportunidad):** La empresa cuenta con amplias posibilidades de ampliar su presencia en el mercado de teléfonos móviles.

1.2.7 ANÁLISIS INTERNO

El objetivo del análisis interno de la empresa es realizar un análisis de los recursos disponibles en la empresa y sus condiciones para contribuir a alcanzar la misión formulada. Esta investigación se ejecuta para identificar fortalezas y debilidades claves en áreas importantes de la empresa.

Ámbito Tecnológico

- **Infraestructura Tecnológica (Fortaleza):** La empresa cuenta con una infraestructura amplia y sólida que permite el desarrollo y la gestión efectiva de aplicativos informáticos que solucionen problemas determinados del negocio.

- **Constante Capacitación (Fortaleza):** En aras de mantener calidad y de lograr una mayor eficiencia en las labores y en el desarrollo de proyectos, la empresa cuenta con una política de capacitaciones, las cuales permiten actualizar o adquirir nuevas habilidades para sus trabajadores.
- **Metodología MEGON (Fortaleza):** Al contar con una metodología con resultados exitosos, la empresa se asegura de producir y gestionar sistemas informáticos de alta calidad y eficientes, siendo un factor clave de éxito de la empresa.

Ámbito de Marketing

- **Grado de Confianza (Fortaleza):** Los clientes de la empresa tienen un buen grado de confianza, pues sabe que reciben calidad, no cualquier producto.
- **Apoyo a Eventos Culturales (Fortaleza):** La empresa continuamente está apoyando eventos culturales, musicales, educativos y de apoyo social a la comunidad peruana.
- **Mala imagen (Debilidad):** Buena parte de la población peruana tiene rechazo a la empresa debido a su alto cobro de llamadas telefónicas y al monopolio que tiene en la telefonía fija, lo cual le permite fijar las tarifas que crea conveniente.

- **Presencia Internacional (Fortaleza):** La empresa es parte de una enorme corporación, la cual tiene una amplia presencia internacional, especialmente en Latinoamérica, con sedes en Brasil, Argentina, Chile y Perú.

Ámbito Organizacional

- **Calidad Total (Fortaleza):** La empresa tiene muy cuenta en factor de calidad en sus servicios y en sus productos tecnológicos. Se aplica la política de mejora continua.
- **Manejo de Personal (Debilidad):** La empresa cuenta con reclamos de ex trabajadores quienes reclaman la reposición de sus empleos, además de empleados actuales los cuales reclaman horas de trabajo sin ser remunerados.
- **Organización del Negocio (Fortaleza):** La empresa, respondiendo a los cambios actuales, cada 6 meses reorganiza su estructura organizacional, permitiendo que su organización sea eficiente frente a las nuevas circunstancias.
- **Gestión de Averías y Reclamos (Debilidad):** A pesar de haber elaborado muchos aplicativos para la gestión eficiente de averías y reclamos, sigue siendo una debilidad pues el usuario final sigue disconforme con la empresa.

- **Liderazgo (Fortaleza):** La presencia de la empresa durante muchos años en el país, aunado a la gran cantidad de productos y servicios que ofrece en gran volumen, han permitido que adquiriera un gran liderazgo.

1.2.8 ANÁLISIS FODA

Fortalezas

- Infraestructura Tecnológica
- Constante Capacitación
- Metodología MEGON
- Grado de Confianza
- Apoyo a Eventos Culturales
- Presencia Internacional
- Calidad Total
- Organización del Negocio
- Liderazgo

Debilidades

- Mala imagen
- Manejo de Personal

Oportunidades

- Demografía del País
- Alta Rentabilidad
- Crecimiento del Uso de Internet
- Masificación del Uso de Celulares

Amenazas

- Posible cambio de sistema económico del país.
- Leyes reguladoras de Osiptel.
- Manifestaciones Públicas.
- Recesión en Perú.

1.2.9 ÁREA DE LA EMPRESA EN ESTUDIO: T-GESTIONA

Descripción: T-Gestiona es Telefónica Gestión de Servicios Compartidos Perú S.A.C. y forma parte de Centros de Servicios Compartidos del Grupo.

Inició sus operaciones el 1° de abril del 2001 y provee servicios integrales de soporte a la gestión a las diversas líneas de negocio de las empresas del Grupo, como un outsourcing, prestando servicios profesionales administrativos y de operación.

Misión: Prestar servicios integrales para satisfacer las necesidades administrativas de todos los negocios del Grupo, así como de clientes externos, liberándolos de gestiones ajenas a su actividad, alcanzando los acuerdos de nivel de servicio, con precios competitivos, actuando de forma profesional, eficiente y confiable, soportados en sistemas de información de última generación, contando con un equipo humano integrado y capacitado, haciendo visibles nuestras cualidades a nuestros.

Visión: Proporcionar servicios profesionales de seguridad con calidad y oportunidad para agregar valor a los negocios de nuestros clientes; a través de la protección adecuada de sus ambientes, activos y personal.

Objetivo: La Protección de la Información tiene como objetivo atender todos los aspectos relativos a la protección física de las materias y documentos clasificados, que involucra al personal, transporte y transmisión de los mismos, incluyendo a la información que fluye por la red informática.

Principales Actividades:

- Emitir políticas que mantengan la seguridad de la información.
- Evaluación de ambientes y sistemas.
- Investigación en casos de fuga de información.
- Operativos para evaluar niveles de riesgo.
- Charlas de inducción.
- Evaluación de personal que ofrece riesgo para la protección de la información

Servicios:

- **Gestión y Desarrollo Humano:** Asisten a las empresas en la gestión de su capital humano, mediante las más actualizadas tecnologías y prácticas existentes en el mercado, adecuadas a las necesidades de cada cliente.
- **Gestión Inmobiliaria:** Cubre desde la definición de las necesidades inmobiliarias de una empresa hasta la adaptación y mantenimiento de sus instalaciones sin barreras geográficas.
- **Seguridad:** Se ofrece una solución integral que comprende la planificación, organización y supervisión permanente de actividades de seguridad para la protección de los recursos de una empresa. Entre

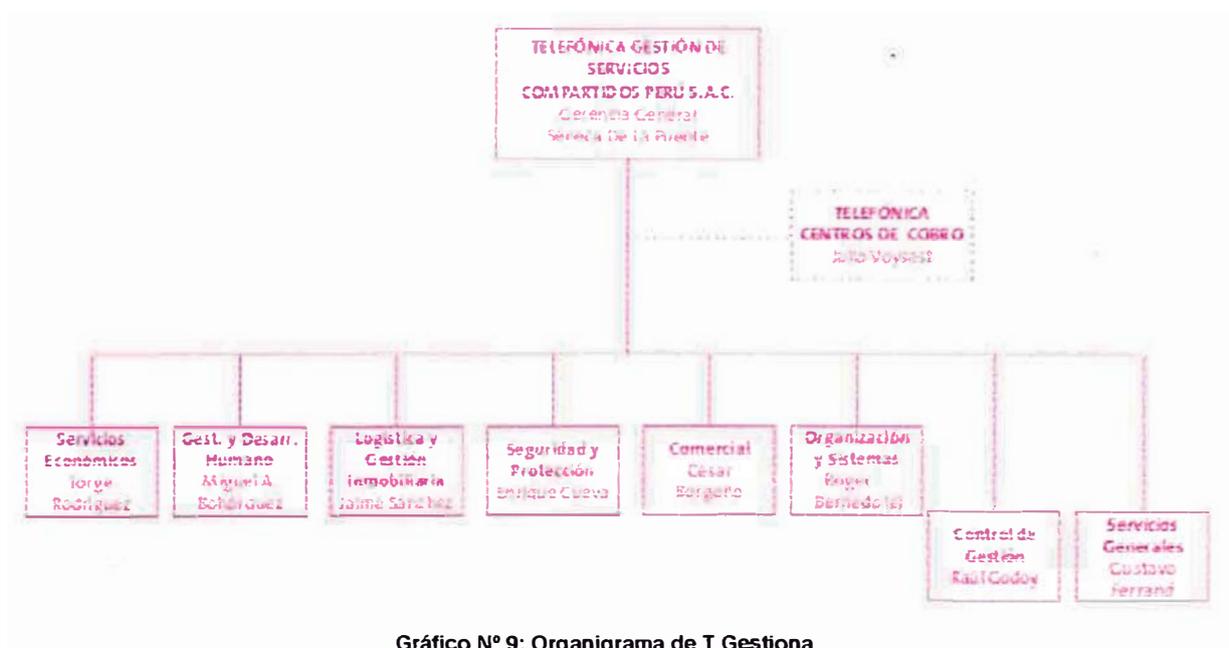
dichos servicios tenemos: Normas Técnicas de Seguridad, Protección de la Información Empresarial, Seguridad Electrónica, Protección contra Incendios, Monitoreo de Alarmas, Gestión de Vigilancia y Guardianía, Seguridad para Eventos. Este es el ámbito del proyecto del presente informe.

- **Recaudación y Cobranza:** Se presta servicios integrales de recaudación gestionando más de 250 establecimientos a nivel nacional y con un sistema informático interconectado que posibilita ofrecer un servicio con actualizaciones en línea. Además se presta servicios de gestión de cobranza con personal especializado en banca, comercio, industria, minería y empresas públicas.
- **Consultoría y Sistemas de Información:** Se optimiza y automatiza los procesos de una empresa. Además se brinda soluciones a la medida, en procesos organizacionales, operativos y de soporte. Algunos de los servicios son: Asesoría para certificación de calidad ISO 9000:2000, Mejora Continua de Procesos de Negocios, Desarrollo y mantenimiento de Sistemas de Información, Consultorías en Planes Estratégicos de Sistemas.
- **Gestión Logística:** Integran los diferentes eslabones de la cadena de suministros; a través de avanzada tecnología sus clientes tienen información cabal en todo momento, sobre el estatus de su mercadería.

- **Contabilidad y Tesorería:** Estos servicios pueden integrarse con facilidad a los procesos de sus clientes y, por ende, ser brindados en forma integral o específica, manteniendo los niveles de oportunidad, confiabilidad y certeza que se requieren y soportados por altos niveles técnicos y con experiencia.

El proyecto abarca básicamente a **T-Gestiona**. Esta incluye entre sus áreas la **Gerencia de Seguridad y Protección (GSP)**, la cual será el área de análisis del presente informe.

Organigrama de T-Gestiona



Organigrama de la GSP:

A continuación se muestra el organigrama de la Gerencia de Seguridad y Protección:

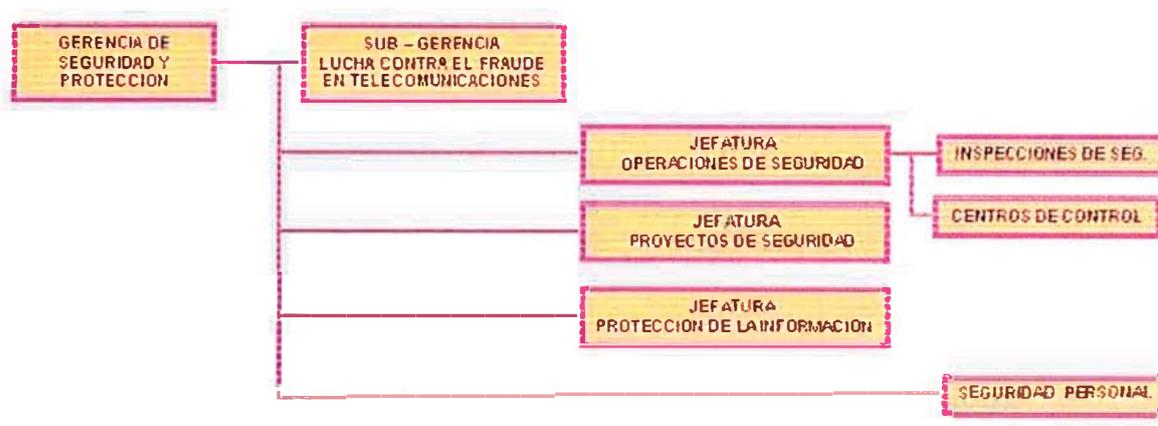


Gráfico N° 10: Organigrama de la Gerencia de Seguridad y Protección

Estructura de la GSP:

La Gerencia de Seguridad y Protección está conformada por 1 Sub-Gerencia, 3 Jefaturas, 1 Supervisión Principal y 1 Central de Alarmas y Teleservicios (CRAT).

En el siguiente cuadro se muestra la estructura de la Gerencia de Seguridad y Protección:

Sub Gerencia	Jefatura	Jefatura	Jefatura	Supervisión	Supervisión
LUCHA CONTRA EL FRAUDE	CENTRO OPERACIONES	PROYECTOS	PROTECCIÓN DE LA INFORMACIÓN	SEGURIDAD PERSONAL	CENTRO DE RECEPCIÓN DE ALARMAS (CRAT)
Objetivo	Objetivo	Objetivo	Objetivo	Objetivo	Propósito
Actividades	Actividades	Actividades	Actividades	Actividades	Ventajas
¿Que es el Fraude en Telecomunicaciones?	Riesgos en Oficinas	Sistema Inteligente (SIS)	Campaña de Difusión	Seguridad Ciudadana	Actividades y Sistemas

Cuadro N° 1: Estructura de la Gerencia de Seguridad y Protección

1.3 DIAGNÓSTICO FUNCIONAL

1.3.1 PRODUCTOS Y SERVICIOS

Seguridad:

- Teleingeniería
- **Ingeniería de Seguridad:** Soluciones de seguridad con un alto nivel de especialización en el uso de telecomunicaciones.

1.3.2 CLIENTES

- Movistar
- Cable Mágico
- Atento
- Terra
- Pléyade
- ONPE
- Edelnor
- Luz del Sur
- Brighstar
- Alcatel

1.3.3 PROVEEDORES

Proveedores de Soluciones de Software

- Cosapisoft
- GMD
- COMSA
- Avances Tecnológicos
- TSNET

Proveedores de Cableado e Instalación

Itete Pert

Proveedores de Tecnologías de la Información

Hewlett Packard (Impresoras, Scanners, etc)

Microsoft

Oracle

EDS: SI Consultoría y Soluciones

SAP (ERP)

META4: Integración de Sistemas

IBM Lotus: Sistemas Workflow

1.3.4 EMPRESAS DEL GRUPO

Empresa del Grupo	Descripción
Atento – Contact Center	Prestación de servicios de atención de las relaciones entre las empresas y sus clientes a través de contact centers o plataformas multicanal.

Cable Mágico	Prestación de servicios de televisión por cable.
Fundación Telefónica	Promoción y gestión de la acción social y cultural del Grupo.
Servicios Editoriales del Perú SAC	Prestación de servicios integrales de edición, fotografía, diseño y pre prensa.
Telefónica Ingeniería de Seguridad	Servicios y sistemas de seguridad.
Telefónica Servicios Digitales	Administración virtual de documentos electrónicos (Virtual Document Management) a través de Internet y las redes de comunicación.
Telefónica Empresas	Proveedor integral de soluciones de comunicaciones y de soporte Internet para empresas.
Terra Networks	Proveedor integral de accesos de internet de banda estrecha y ancha. Edición y comercialización del Portal www.terra.com.pe
T-Gestiona	Soluciones en tercerización de servicios administrativos: Recursos Humanos, Gestión Inmobiliaria, Seguridad, Recaudación, Organización y Sistemas, Gestión Logística, Contabilidad y Tesorería.

T-Móviles SAC	Prestación de servicios de telefonía móvil y buscapersonas.
TPI Páginas Amarillas	Edición y comercialización de directorios telefónicos.
TUMSAC	Servicio de mensajería en general, local, nacional e internacional.

Cuadro N° 2: Empresas del Grupo

CAPÍTULO 2

MARCO TEÓRICO

2.1 SEGURIDAD DE LA INFORMACIÓN

2.1.1 CONCEPTOS GENERALES

2.1.1.1 PRIVACIDAD

Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán transmitidas a otros.

2.1.1.2 SEGURIDAD

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser manipulados, modificados, destruidos o simplemente divulgados.

En el caso de la información de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

2.1.1.3 INTEGRIDAD

Este concepto está referido a que los registros de la información se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

2.1.1.4 ACCESO

Es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

2.1.1.5 AMENAZA

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal o servidor, o causar la difusión no autorizada de información confiada.

Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

2.1.1.6 INCIDENCIA

Es todo suceso que atenta contra la seguridad de información de una empresa.

Las inspecciones PIE consisten en el seguimiento in situ (en las áreas de trabajo) de la aplicación de pautas de conducta mínimas de protección de la información por parte de los trabajadores, su resultado es el conjunto de incidencias ocurridas y registradas.

2.1.2 SEGURIDAD DE LA INFORMACIÓN

2.1.2.1 ACCESOS

La seguridad de la información tiene dos aspectos. El primero consiste en negar el acceso a los datos a aquellas personas que no tengan derecho a ellos, al cual también se le puede llamar protección de la privacidad, si se trata de datos personales, y mantenimiento de la seguridad en el caso de datos institucionales.

Un segundo aspecto de la protección es garantizar el acceso a todos los datos importantes a las personas que ejercen adecuadamente su privilegio de acceso, las cuales tienen la responsabilidad de proteger los datos que se les ha confiado.

En general, la protección de los datos requiere ejercer un control sobre la lectura, escritura y empleo de esa información. Para obtener mayor eficiencia en la protección se debe tener siempre presente la protección de los datos, el mantenimiento de la privacidad y la seguridad del secreto.

2.1.2.2 DESTRUCCIÓN

Sin adecuadas medidas de seguridad las empresas pueden estar a merced no sólo de la destrucción de la información sino también de la destrucción de su equipo informático.

La destrucción del equipo puede darse por una serie de desastres como son: incendios, inundaciones, sismos, o posibles fallas eléctricas, etc. Esto también debe ser reportado como incidencia.

2.1.2.3 INFIDENCIA

La revelación o infidencia es otra forma que utilizan los malos empleados para su propio beneficio. La información, que es de carácter confidencial, es filtrada o vendida a personas ajenas a la institución, incluso a la competencia.

2.1.2.4 MODIFICACIONES

La importancia de los datos que se modifican de forma ilícita, está condicionada al grado en que la organización depende de los datos para su funcionamiento y toma de decisiones. Para ello, siempre es recomendable hacer copias de seguridad.

2.1.3 POLÍTICAS DE SEGURIDAD

2.1.3.1 INTRODUCCIÓN

Actualmente, muchas empresas compran soluciones costosas y afamadas, como software antivirus, firewall, software de filtrado de contenido, sistemas antispam, e incluso redes privadas virtuales. Y aun así, son atacados por hackers y crackers, e incluso por ex trabajadores y trabajadores (boicot).

El mayor problema radica en que muchos proveedores de seguridad informática se limitan a vender productos sin tener en cuenta las características de los clientes, sus vulnerabilidades y las políticas que deberían implementar. Esto hace que la compañía crea que está protegida cuando en realidad tiene huecos importantes de seguridad.

No solo se requiere de tecnología, también es necesario definir **políticas de seguridad**. Las empresas deben ser conscientes de la importancia de estas políticas, muchas creen que lo más importante son las herramientas, y que lo demás es secundario.

2.1.3.2 ¿CÓMO DESARROLLAR POLÍTICAS DE SEGURIDAD?

Estas políticas son las reglas y procedimientos que regulan la forma como una organización previene y enfrenta los riesgos de su infraestructura tecnológica (equipos de cómputo y sus periféricos, software y el activo más importante, la información).

Estas políticas no deberían ser opcionales. En mi opinión, todas las organizaciones, sin importar su tamaño, no sólo deben definir las, sino también generar una estrategia de concientización e incluirlas en los contratos laborales (deben ser de cumplimiento obligatorio).

Los proveedores de soluciones tecnológicas sugieren unos pasos para que cualquier empresa desarrolle sus propias políticas de seguridad:

- **Identificar los activos.** Valorar cada activo (incluyendo los intangibles), estableciendo los niveles de protección para cada uno.

- **Identificar las amenazas.** Pueden ser amenazas externas (virus, spam, gusanos, ataques de piratas informáticos, espionaje industrial) o internas (venganzas de ex empleados, uso indebido de Internet y los sistemas informáticos).

- **Medir los riesgos.** ¿Qué tan probable es que sucedan ciertos hechos puntuales, y cuánto daño pueden causar? Al calcular los daños en cifras no sólo se debe tener en cuenta el valor de los equipos o las aplicaciones, sino el de la información y otros intangibles.

- **Armar un equipo de trabajo.** Considerar, además de los líderes del área de sistemas, un asesor jurídico, alguien del área de recursos humanos, y un representante de cada área de la organización que se encargue de ayudar a identificar las amenazas.

- **Establecer políticas.** Con base en la información recolectada, se pueden redactar los procedimientos y normas. El resultado debe ser un documento conciso, fácil de entender por parte de los empleados y que no vaya al extremo de bloquear la productividad en aras de la seguridad.

- **Implementar dichas políticas.** Definir los responsables de la difusión y el cumplimiento de las nuevas pautas, y señalar los procedimientos para controlar que esto se cumpla.

2.1.3.3 INVERSIÓN AL IMPLANTAR POLÍTICAS DE SEGURIDAD

La implementación de estas políticas puede demandar algunos recursos, pero en muchos casos no se requiere invertir más, sino reasignar recursos. Además, la inversión se recupera con los beneficios.

Las políticas, en conjunto con un plan de concientización de usuarios, son la herramienta más importante para mitigar los riesgos de seguridad de la información, pues ayudan a garantizar la confidencialidad necesaria de la información, mejoran su disponibilidad y confiabilidad, y ayudan a minimizar el riesgo de pérdida de reputación, tiempo, dinero, productividad y acciones legales

2.1.3.4 NORMAS INTERNACIONALES

Normas internacionales, como la BS 7799 y la ISO 17799, establecen las pautas que las empresas deben seguir. Algunas son:

- Toda empresa debe tener un responsable de la seguridad de la información.

- Toda la información de la compañía es confidencial.

- Todos los recursos son para uso exclusivo en el trabajo asignado, no para asuntos personales.

- Todo el software instalado debe estar debidamente licenciado.

- Todo documento que no se requiera debe ser debidamente archivado o destruido.

- El acceso a la información, en archivos físicos o electrónicos, debe restringirse exclusivamente a los que la necesitan.
- Se deben definir los procesos para recuperación de desastres.
- Se debe definir un esquema de clasificación e identificación de la información para controlar su integridad, confidencialidad y disponibilidad.

2.1.4 INFORMACIÓN CONFIDENCIAL

La Real Academia de la Lengua Española define “confidencial” como “que se hace o se dice en confianza o con seguridad recíproca entre dos o más personas”, y “confidencialidad” como “la cualidad de confidencial”. Así pues, la empresa tiene la libertad de calificar su información como confidencial, incluyendo documentos, que a su juicio, influya directa o indirectamente en el desarrollo del negocio: estrategias empresariales, métodos de negocio, contratos, propiedad intelectual, patentes, desarrollo de nuevos productos, etc.

Esta información confidencial ha de gozar de una protección especial, tendente a evitar su filtración, divulgación o difusión a terceros, acciones que pueden causar graves perjuicios a su empresa (imaginemos por ejemplo, que una

determinada estrategia empresarial tendente a posicionar en el mercado una determinada empresa, es filtrada y difundida previa y fraudulentamente a la competencia, lo que impide al empresario el posicionamiento deseado).

Respecto a la Protección de la Información Empresarial, dentro de la propia empresa hay que distinguir entre los trabajadores y el personal de alta dirección, que por razón de su puesto y funciones, accede o trata dicha Información.

En cuanto al Personal de Alta Dirección, y dado que por razón de su cargo acceden a información especialmente sensible y/o confidencial, existe la obligación expresa de mantener la confidencialidad y secreto de las informaciones a las que tiene acceso por razón de su cargo, siendo práctica habitual el firmar acuerdos específicos de confidencialidad junto con los contratos de trabajo, bien a través de una cláusula específica de confidencialidad en los contratos, o bien incluyendo un pacto o acuerdo de confidencialidad como anexo al contrato principal de trabajo.

2.1.5 OTROS MEDIOS DE PROTECCIÓN INTERNA DE LA INFORMACIÓN CONFIDENCIAL

Es recomendable establecer las siguientes medidas de protección:

-Limitar el acceso a la información confidencial. Es decir, permitir el acceso a dicha información sólo al personal que por razón de su cargo o funciones es necesario que acceda a dicha información, no permitiendo tal acceso al resto del personal.

-Establecer medidas técnicas que permitan la visualización o tratamiento de información confidencial (por ejemplo: uso de contraseñas para el acceso a los documentos, criptografía, etc.).

-Mantener/Almacenar los documentos confidenciales en soporte papel, en armarios que se encuentren cerrados bajo llave o cajas fuertes, a las que sólo tengan acceso las personas autorizadas.

-Realizar de copias de seguridad que eviten la pérdida de información confidencial o sensible en caso de catástrofe, guardando una copia fuera de las instalaciones principales de la empresa.

2.1.6 PROTECCIÓN DE LA INFORMACIÓN EN CASOS DE OUTSOURCING

Cuando una empresa vaya a encargar la prestación de un determinado servicio, que implique el tratamiento o acceso a información confidencial por parte de terceras empresas (como es el caso de nuestra empresa en análisis), es

recomendable incluir en el contrato de prestación de servicios, una cláusula específica de confidencialidad, o bien, firmar directamente con cada una de las personas que accedan a dicha información, pactos o acuerdos de confidencialidad específicos.

2.2 METODOLOGÍA DE DESARROLLO MEGON

La empresa viene utilizando desde hace ya varios años la metodología **MEGON**, que le ha dado excelentes resultados. Los proveedores contratados por la empresa también siguen esta metodología para el desarrollo de aplicativos para la empresa.

2.2.1 MODELO DE GESTIÓN MEGON

Gestión Orientada al Cliente

En la gestión de proyectos, desde una perspectiva tradicional, predomina la orientación técnica: una gestión basada en la consecución de objetivos de productividad, en la que el cliente asume un papel de espectador. Desde esta época el cliente acepta o rechaza aunque en pocas ocasiones participa.

Pero si se quieren asumir cotas más altas de servicio, es necesario diseñar un sistema donde el cliente tenga un papel esencial, el de la participación y el compromiso. La gestión de proyectos ha de reorientarse hacia un modelo integrado de gestión de clientes y proyectos. Así pues, este modelo de gestión se fundamenta en:

- Unos criterios únicos de relación con los clientes,
- Unos criterios únicos de calidad.

El punto de control, una herramienta de gestión

Es un modelo único de gestión, es preciso que existan puntos de control que aseguren la calidad y permitan la gestión de los diferentes proyectos. De esta manera el punto de control se convierte en una herramienta que:

- Crea un lenguaje común.
- Potencia el diálogo y la participación.
- Proporciona herramientas para medir la producción y la calidad.
- Es independiente de la tecnología utilizada.

Los roles

Quien gestiona es una cuestión que también hay que resolver. En una organización dinámica, el trabajo no puede estar ligado a individuos sino a los roles que éstos ejercen. De esta manera cada tarea queda asignada a un rol, pero el individuo puede realizar uno, dos o más roles.

Los roles determinados por el modelo MEGON son: Gestor de Cliente, Jefe del Proyecto, Analista, Diseñador Interno, Programador, Cliente y Grupos de Apoyo.

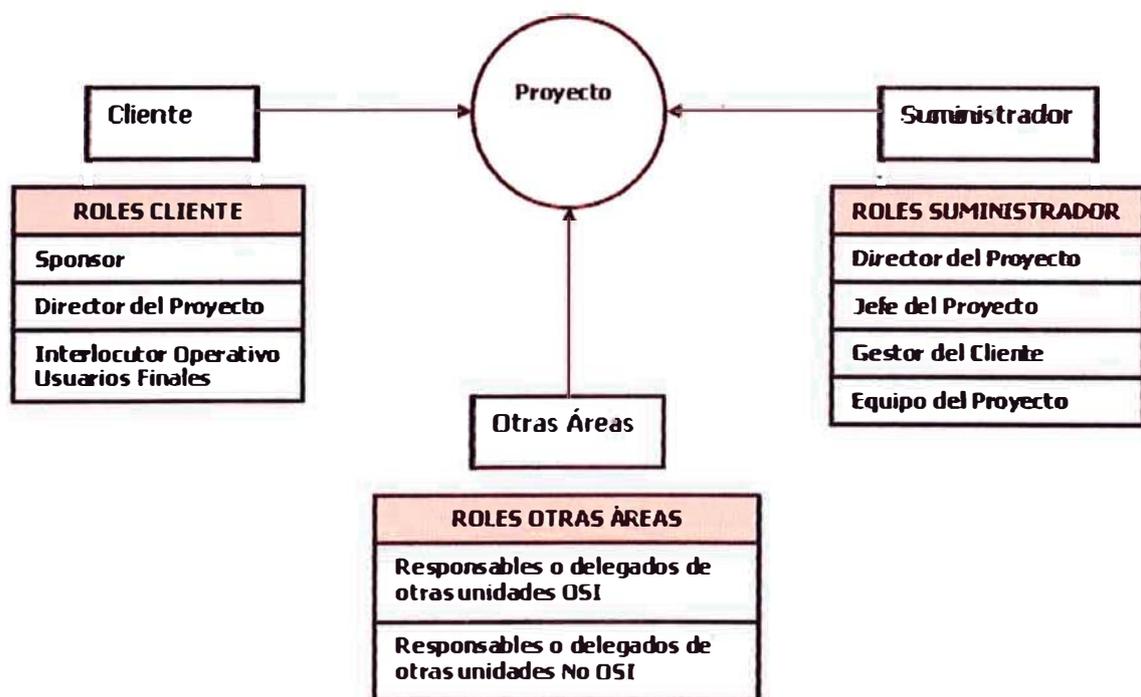


Gráfico N° 11: Roles existentes en el Modelo MEGON

2.2.2 ESTRUCTURA DEL MEGON

Este marco propone 9 fases agrupados en 3 bloques: cada fase está compuesta de actividades, puntos de control y entregables.

Bloque 1: Planificación del Sistema de Información del Cliente.

Identificación, definición y priorización de la cartera de Proyectos de Sistemas de Información.

Bloque 2: Provisión de Soluciones. Desde el análisis de los requisitos hasta la implementación del proyecto a desarrollar.

Bloque 3: Apoyo a Soluciones Operativas. Mejoramiento del proyecto implementado.

El primer y tercer bloque involucran actividades propias de la gestión de clientes, mientras que el segundo bloque contempla de gestión de proyectos.

El contenido de cada bloque se estructura en diversas fases. Cada una de ellas agrupa una serie de actividades necesarias para la consecución de objetivos. Al final de cada fase encontramos un punto de control donde podemos comprobar que se han alcanzado los resultados esperados.

2.2.3 HITOS Y ENTREGABLES

Los productos o entregables que emita el equipo del proyecto en determinado momento (hitos) deben considerarse versiones incompletas y significativamente perfectible a medida que avanza el proyecto. Sin embargo la emisión de estas versiones resulta necesaria para realizar un control de resultados y aportar retroalimentación.

Los productos o entregables se emiten mediante versiones a lo largo de todo el proyecto (cada versión presenta el nivel de madurez de conceptos logrado por el equipo del proyecto en un momento dado)

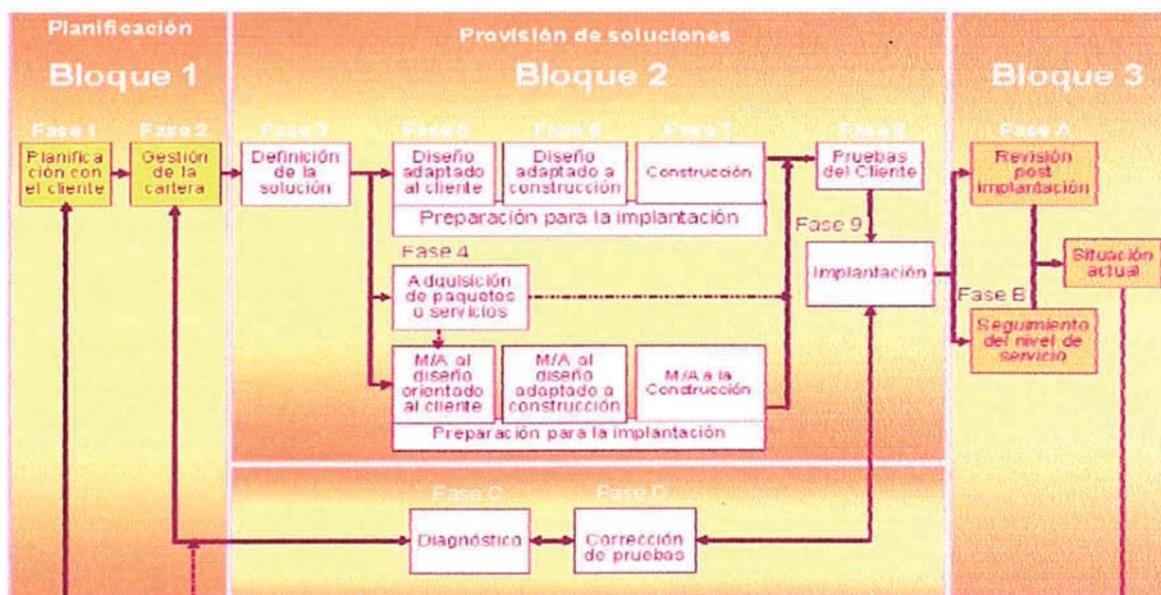




Gráfico Nº 12: Etapas de la Metodología MEGON

BLOQUE	FASE	HITO	ENTREGABLE CLAVE	ARMONIZACIÓN ROLES RESPONSABLE POR FASE			
				MEGON	SUMINISTRO	ESQUEMA SWF	
						OSI	SWF
B1: PLANIFICACIÓN DE S.I. DEL CLIENTE	B1F1	Aceptación Plan SSII del Cliente	PR01011 Plan de S.I. del Cliente	Gestor del Cliente	Gestor del Cliente	Gestor Informático	-
	B1F2	Lanzamiento de Proyectos de Cartera	PR01020 Solicitud del Cliente	Gestor del Cliente	Gestor del Cliente	Gestor Informático	-
B2: PROVISIÓN DE SOLUCIONES	B2F3	Aceptación Propuesta de la Solución y Plan de Trabajo	PR11020 Propuesta de la Solución PR11020 Propuesta de la Solución	Director del Proyecto Gestor del Cliente	Director del Proyecto Gestor del Cliente Jefe de Proyecto	Director OSI Gestor Informático Analista de Negocio	Especialista (coordinación y seguimiento)

			Solución PR110200 Plan de Trabajo	Jefe de Proyecto			
B2F4	Aceptación Adquisición de Paquetes o Servicios	Instalación del Paquete o Servicio	PR31011 Paquete o servicio instalado	Jefe de Proyecto Analista Negocio	Jefe de Proyecto Consultor	Analista de Negocio	Especialista
B2F5	Diseño Adaptado al Cliente	Aceptación Diseño Adaptado al cliente	PR21011 Especific. de Requisitos y Diseño Externo PR11011 Modelo de Datos y Procesos PR21020 Manual de Usuario PR21031 Plan de Pruebas del Cliente	Jefe de Proyecto Analista Negocio	Jefe de Proyecto Consultor	Analista de Negocio	Especialista
B2F6	Diseño Adaptado a la Construcción	Aprobación Diseño adaptado a la Construcción.	PR22030 Diseño de Procesos y Archivos Físicos PR22040 Manual de Explotación PR22041 Manual de Instalación y Configuración	Jefe de Proyecto Analista Técnico	Jefe de Proyecto Analista	Analista de Negocio (coordinación y seguimiento)	Especialista (coordinación y seguimiento) Analista
B2F7	Construcción	Aprobación Software Construido y Probado	PR23020 Software Producido	Jefe de Proyecto Analista Técnico	Jefe de Proyecto Analista	Analista de Negocio (coordinación y seguimiento)	Especialista (coordinación y seguimiento) Analista
B2F8		Aceptación	PR81020 Informe	Gestor del	Gestor del	Gestor	Especialista

	Pruebas de Cliente	Pruebas del Cliente Aceptación Plan de Implantación	de Pruebas del Cliente PR81031 Plan de Implantación	Proyecto Jefe de Proyecto Analista Técnico	Proyecto Jefe de Proyecto Analista	Informático Analista de Negocio	(coordinación y seguimiento) Analista Líder Test
	B2F9 Implantación	Aceptación Implantación del Sistema	PR82011 Software distribuido a Producción	Director del Proyecto Gestor del Proyecto Jefe del Proyecto	Director del Proyecto Gestor del Proyecto Jefe del Proyecto	Director OSI Gestor de Informático Analista de Negocio (coordinación y seguimiento)	Especialista (coordinación y seguimiento)
B2: MANTENIMIENTO CORRECTIVO	B3FC Diagnóstico	Aprobación de la Solución Correctiva	PR51020 Propuesta de la Solución Correctiva	Jefe de Proyecto Analista Técnico	Jefe de Proyecto Analista	Analista de Negocio	Especialista Analista
	B3FD Corrección y Pruebas	Aceptación del Software Corregido	PR23020 Software Producido	Jefe de Proyecto Analista Técnico	Jefe de Proyecto Analista	Analista de Negocio (coordinación y seguimiento)	Especialista (coordinación y seguimiento) Analista
B3: SOPORTE A SOLUCIONES OPERATIVAS	B3FA Revisión post implantación	Revisión post implantación	PR82020 Informe de la Situación Actual PR91011 Análisis Final del Proceso de Construcción	Gestor del Cliente	Gestor del Cliente	Gestor Informático	-
	B3FB Seguimiento del Nivel de Servicio	Aceptación del Nivel de Servicio	PR82020 Informe de la Situación Actual	Director del Proyecto Gestor del Proyecto	Director del Proyecto Gestor del Proyecto	Director OSI Gestor de Informático Analista de	Director / Responsable Especialista (coordinación

				Proyecto Jefe del Proyecto	Jefe del Proyecto	Negocio (coordinación y seguimiento)	y seguimiento)
--	--	--	--	----------------------------------	-------------------	---	-------------------

CAPÍTULO 3

PROCESO DE TOMA DE DECISIONES

3.1 PLANTEAMIENTO DEL PROBLEMA

Para reportar las incidencias de protección de la información, se realiza un proceso manual y extenso: el personal de vigilancia genera esta información en formato Excel, y es enviada a través de correo electrónico y la red (carpetas compartidas por cada local), involucrando un alto riesgo en cuanto a manipulación y alteración de datos. Además, cada local llena el formato de manera diferente, lo cual complica la consolidación de las incidencias, y más aún, su análisis.

El proceso actual para la identificación de los trabajadores con riesgos PIE es lento generando que los informes a los mandos del área o gerencia se entreguen casi con un mes de retraso.

3.2 ALTERNATIVAS DE SOLUCIÓN

Se propuso desarrollar un software que automatice estos procesos, para mejorar la confiabilidad de la información y el tratamiento de las incidencias PIE, como: incidencias por trabajador, incidencias por área y reportes estadísticos mensuales o del tiempo que se requiera.

No se considera como alternativa el desarrollo in-house debido a que una política establece que el desarrollo de software debe ser mercerizado. Por ello, se presentaron diferentes proveedores como Cosapisoft, GMD y COMSA, cada uno con su propuesta de plan de trabajo del proyecto. En el siguiente cuadro se muestran los resultados:

Característica	Alt. 1: CosapiSoft	Alt. 2: COMSA	Alt. 3: GMD
Características Técnicas			
Tipo de Desarrollo	Desarrollo a Medida	Desarrollo a Medida	Adquisición de Software Desarrollado (Licenciamiento)
Descripción	Solución Lotus	Solución Lotus	Solución Lotus
Tipo de Plataforma	Centralizada	Centralizada	Centralizada

Arquitectura	3 Capas	3 Capas	2 Capas
Sistema Operativo de Base de Datos	Windows 2000	Windows NT	Windows NT
Base de Datos	Lotus Domino	Lotus Domino	Lotus Domino
Servidor de Aplicaciones	SI	SI	SI
Software de Desarrollo en Servidor de Aplicaciones	SI	SI	NO
Máquina Cliente	PC IBM	PC Compatible	PC IBM
Software en Cliente	Internet Explorer 6.0	Internet Explorer 5.5	Internet Explorer 5.5
Tipo de Tecnología	Lotus Notes	Lotus Notes	Lotus Notes
Características sobre el Negocio			
Conocimiento y Experiencia en el Desarrollo de Software para	SI	SI	SI

Empresas Privadas			
Experiencia en el Desarrollo de Sistemas de PIE	NO	SI	SI

Cuadro N° 3: Características Técnicas de las Alternativas

3.3 METODOLOGÍA DE SOLUCIÓN

Para analizar cual de las alternativas es la más conveniente, se analizó funcionalmente y mediante una evaluación de costos implicados del proyecto por alternativa.

La evaluación funcional se dio en una reunión entre la Gerencia y los usuarios implicados. Se muestra un cuadro con los criterios analizados y su peso asignado.

Criterio de Análisis	Motivo de su Inclusión
Funcionalidad (Peso: 15%)	Criterio que considera cuánto de la funcionalidad necesitada es cubierta por la alternativa. Para ello, MEGON provee documentos de control para la

	funcionalidad, por cada módulo del aplicativo.
Conocimiento del Negocio (Peso: 20%)	Criterio que considera el conocimiento que tiene el proveedor con respecto al negocio.
Costo del Proyecto (Peso: 15%)	Criterio que considera los costos acarreados del proyecto.
Imagen y Experiencia del Proveedor (Peso: 10%)	Criterio que considera la experiencia del proveedor en el desarrollo de tipo de aplicativo necesitado. Para ello analizan el listado de cada proveedor de su experiencia en diversos proyectos.
Estabilidad Financiera del Proveedor (Peso: 15%)	Criterio que considera la estabilidad en el aspecto financiero del proveedor, pues influye para tener la confiabilidad de un producto terminado de calidad y con altos niveles de servicio.
Tiempo del Proyecto (Peso: 10%)	Criterio que considera el tiempo de duración del proyecto.
Servicio Post Venta (Peso: 10%)	Criterio que considera la atención post venta del proveedor, para mantenimiento, help desk y mejoras, respecto al aplicativo.

Cuadro N° 4: Factores Técnicos para Selección de Alternativa

La evaluación financiera se basó en los costos del proyecto por proveedor. Se muestra los cuadros de costos:

SISTEMA DE PROTECCIÓN DE LA INFORMACIÓN EMPRESARIAL - COSAPIDATA			
CUADRO DE COSTOS - 2005			
Descripción	Valor Mensual	Número de Meses	Total
Planilla			
Personal	54,132.00	2	108,264
Software	0.00	2	0
TOTAL A			108,264
Infraestructura y Servicios			
Equipos de Cómputo y Muebles	2,000.00	2	4,000
Servicios de Mantenimiento e Instalación	500.00	2	1,000
Suministros	350.00	2	700
TOTAL B			5,700
SUB TOTAL (A+B)			113,964
G. Administrativos (sobre Sub total A y B)		5%	5,698
Contingencia (sobre Sub total y Gastos Administrativos)		3%	3,590
Utilidad (en base a gastos sobre A)		15%	17,563
Total			140,815
IGV		19%	26,755
Gran Total		S/.	167,570
		US\$	50,473
Costo Mensual		S/.	83,785
		US\$	25,236

Cuadro N° 5: Cuadro de Costos Alternativa 1

SISTEMA DE PROTECCIÓN DE LA INFORMACIÓN EMPRESARIAL - COMSA

CUADRO DE COSTOS - 2005

Descripción	Valor Mensual	Número de Meses	Total
Planilla			
Personal	53,670.00	2	107,340
Software	0.00	2	0
TOTAL A			107,340
Infraestructura y Servicios			
Equipos de Cómputo y Muebles	2,200.00	2	4,400
Servicios de Mantenimiento e Instalación	550.00	2	1,100
Suministros	300.00	2	600
TOTAL B			6,100
SUB TOTAL (A+B)			113,440
G. Administrativos (sobre Sub total A y B)		5%	5,672
Contingencia (sobre Sub total y Gastos Administrativos)		3%	3,573
Utilidad (en base a gastos sobre A)		15%	17,413
Total			140,099
IGV		19%	26,619
Gran Total		S/.	166,717
		US\$	50,216
Costo Mensual		S/.	83,359
		US\$	25,108

Cuadro N° 6: Cuadro de Costos Alternativa 2

SISTEMA DE PROTECCIÓN DE LA INFORMACIÓN EMPRESARIAL - GMD

CUADRO DE COSTOS - 2005

Descripción	Valor Mensual	Número de Meses	Total
Planilla			
Personal	56,950.00	2	113,900
Software	0.00	2	0
TOTAL A			113,900
Infraestructura y Servicios			
Equipos de Cómputo y Muebles	2,700.00	2	5,400
Servicios de Mantenimiento e Instalación	420.00	2	840
Suministros	320.00	2	640
TOTAL B			6,880
SUB TOTAL (A+B)			120,780
G. Administrativos (sobre Sub total A y B)		5%	6,039
Contingencia (sobre Sub total y Gastos Administrativos)		3%	3,805
Utilidad (en base a gastos sobre A)		15%	18,477
Total			149,101
IGV		19%	28,329
Gran Total		S/.	177,430
		US\$	53,443
Costo Mensual		S/.	88,715
		US\$	26,721

Cuadro N° 7: Cuadro de Costos Alternativa 3

3.4 TOMA DE DECISIONES (SELECCIÓN DE LA ALTERNATIVA ESCOGIDA)

En la reunión mencionada, se analizó cada criterio por proveedor, estableciéndose un cuadro de decisiones ponderado, cuya valoración van desde 1 a 10, el cual se muestra a continuación:

Criterios	Peso	CosapiSoft	COMSA	GMD
Funcionalidad	15%	9	10	10
Conocimientos del Negocio	20%	8	10	10
Costo del Proyecto	15%	8	8	7
Imagen y Experiencia del Proveedor	10%	5	6	5
Estabilidad Financiera del Proveedor	15%	6	6	7
Tiempo del Proyecto	15%	8	8	8
Servicio Post Venta	10%	6	7	7
Puntaje Total	100%	7.35	8.10	8.00

Cuadro N° 8: Selección de la Alternativa

En el cuadro mostrado anteriormente, el criterio con mayor peso en la evaluación es el grado de conocimiento del negocio que tiene el proveedor.

Después siguen la funcionalidad del sistema, el costo y tiempo del proyecto, y la estabilidad financiera del proveedor.

Además, en base al cuadro resumen de costos por proveedor:

	CosapiData	COMSA	GMD
Costo Total	25236	25108	26721
Mensual en Dólares			

Cuadro N° 9: Selección de la Alternativa

Al evaluar las 3 propuestas, teniendo en cuenta el cuadro comparativo de ponderación mostrado anteriormente y el cuadro resumen de costos, se optó por la **alternativa 2 (COMSA)**, que cuenta con amplia experiencia en el negocio, el mejor precio, notable estabilidad financiera y un buen tiempo para el proyecto, además de los menores costos por mes del proyecto.

3.5 ESTRATEGIAS ADOPTADAS

3.5.1 CRONOGRAMA DEL PROYECTO (DIAGRAMA GANTT)

Se muestra a continuación el plan del proyecto:

Id	Nombre de tarea	Duración	Esfuerzo	Inicio	Fin	Recursos
1	SI-PIE	50 días	179 días	lun 27/06/05	mar 06/09/05	
2	Gerencia del Proyecto	45 días	9 días	lun 27/06/05	mar 30/08/05	GF[20%]
3	Análisis de los requisitos	4 días	12 días	lun 27/06/05	jue 30/06/05	Ap1,AF,Ap2
4	HITO: Entrega de Plan de Trabajo	0 días	0 días	jue 30/06/05	jue 30/06/05	GP
5	Diseño Adaptado al Cliente	3 días	9 días	vie 01/07/05	mar 05/07/05	Ap1,AF,Ap2
6	HITO: Entrega Diseño Adaptado al Cliente	0 días	0 días	mar 05/07/05	mar 05/07/05	GP
7	Diseño Adaptado a la Construcción	3 días	9 días	mié 06/07/05	vie 08/07/05	Ap1,AF,Ap2
8	HITO: Entrega Diseño Adaptado a la Construcción	0 días	0 días	vie 08/07/05	vie 08/07/05	GP
9	Construcción de Componentes	22 días	76 días	lun 11/07/05	jue 11/08/05	
10	Administración	11 días	22 días	lun 11/07/05	lun 25/07/05	
11	Definición de BD's	0.5 días	1 día	lun 11/07/05	lun 11/07/05	P1,AF
12	Registro y mantenimiento de Negocios	1 día	2 días	lun 11/07/05	mar 12/07/05	P1,AF
13	Registro y mantenimiento de Pisos	1 día	2 días	mar 12/07/05	mié 13/07/05	P1,AF
14	Registro y mantenimiento de Módulos por Piso	1 día	2 días	mié 13/07/05	jue 14/07/05	P1,AF
15	Registro y mantenimiento de Locales	1 día	2 días	jue 14/07/05	vie 15/07/05	P1,AF
16	Registro y mantenimiento de Vigilantes	1 día	2 días	vie 15/07/05	lun 18/07/05	P1,AF
17	Registro y mantenimiento de Inventarios	2 días	4 días	lun 18/07/05	mié 20/07/05	P1,AF
18	Registro y mantenimiento de Tipos de Incidencias	1 día	2 días	mié 20/07/05	jue 21/07/05	P1,AF
19	Asociación de Tablas	2 días	4 días	jue 21/07/05	lun 25/07/05	P1,AF
20	Seguridad de Administración	0.5 días	1 día	lun 25/07/05	lun 25/07/05	P1,AF
21	Incidencias del Trabajador	18 días	18 días	lun 11/07/05	vie 05/08/05	
22	Definición de las bd's	0.5 días	0.5 días	lun 11/07/05	lun 11/07/05	Ap1
23	Desarrollo del formulario de incidencias del trabajador	3 días	3 días	lun 11/07/05	jue 14/07/05	Ap1
24	Registro de incidencias del trabajador	4 días	4 días	jue 14/07/05	mié 20/07/05	Ap1
25	Interfaz gráfica de incidencias del Trabajador	1 día	1 día	mié 20/07/05	jue 21/07/05	Ap1
26	Reporte de Incidencias por fecha	2.5 días	2.5 días	jue 21/07/05	lun 25/07/05	Ap1
27	Nº de incidencias por fecha	2 días	2 días	mar 26/07/05	mié 27/07/05	Ap1
28	Nº de verificaciones realizadas por fecha	2 días	2 días	lun 01/08/05	mar 02/08/05	Ap1
29	Personal con mayor incidencia	1.5 días	1.5 días	mié 03/08/05	jue 04/08/05	Ap1
30	Personal con mayor incidencia por verificación	1.5 días	1.5 días	jue 04/08/05	vie 05/08/05	Ap1
31	Incidencias del Area	16 días	16 días	lun 11/07/05	mié 03/08/05	
32	Desarrollo del formulario de incidencias del area	3 días	3 días	lun 11/07/05	mié 13/07/05	Ap2
33	Registro de incidencias del Area	3 días	3 días	jue 14/07/05	lun 18/07/05	Ap2
34	Interfaz grafica de incidencias del area	1 día	1 día	mar 19/07/05	mar 19/07/05	Ap2
35	Reporte de incidencias por fecha	2 días	2 días	mié 20/07/05	jue 21/07/05	Ap2
36	Nº de Incidencias por fecha	2 días	2 días	vie 22/07/05	lun 25/07/05	Ap2
37	Nº de verificaciones realizadas por fecha	2 días	2 días	mar 26/07/05	mié 27/07/05	Ap2
38	Area con mayor incidencia	2 días	2 días	lun 01/08/05	mar 02/08/05	Ap2
39	Area con mayor incidencia por verificación	1 día	1 día	mié 03/08/05	mié 03/08/05	Ap2
40	Interfaz con el Sistema de Control de Acceso	4 días	8 días	lun 08/08/05	jue 11/08/05	
41	Interfaz	4 días	8 días	lun 08/08/05	jue 11/08/05	Ap1,AF
42	Identificación de Usuarios con Incidencias	6 días	12 días	jue 04/08/05	jue 11/08/05	
43	Obtención de Datos del Trabajador asignado a	6 días	12 días	jue 04/08/05	jue 11/08/05	Ap2,P1
44	HITO: Fin de Construcción	0 días	0 días	lun 11/07/05	lun 11/07/05	GP
45	Pruebas integrales	10 días	30 días	vie 12/08/05	jue 25/08/05	Ap1,Ap2,P1
46	HITO: Aceptación Pruebas del Cliente	0 días	0 días	jue 25/08/05	jue 25/08/05	GP
47	Diseño Grafico	5 días	5 días	lun 18/07/05	vie 22/07/05	Dis
48	Documentacion entregables	24 días	12 días	lun 27/06/05	lun 01/08/05	Doc[50%]
49	Capacitación a Usuarios	3 días	3 días	vie 26/08/05	mar 30/08/05	Ap1
50	Capacitación Administradores	3 días	3 días	vie 26/08/05	mar 30/08/05	Ap2
51	Testing	5 días	5 días	vie 26/08/05	jue 01/09/05	P1
52	Puesta en marcha	3 días	6 días	vie 02/09/05	mar 06/09/05	Ap1,Ap2
53	Hito de Control: Fin	0 días	0 días	mar 06/09/05	mar 06/09/05	GP

3.5.2 DESCRIPCIÓN GENERAL DEL SISTEMA

El sistema permite automatizar el proceso manual de identificación de los trabajadores con riesgos o incidencias, resultado de las inspecciones de Protección de la Información Empresarial, un control exacto de los resultados de las inspecciones realizadas, además proporciona consultas y reportes sobre las incidencias registradas.

La Subgerencia de Lucha contra el Fraude (perteneciente a la Gerencia de Seguridad y Protección GSP) es la involucrada, a ella se le remiten los reportes.

3.5.3 OBJETIVO DEL SISTEMA

- Automatizar el proceso manual de Identificación de los trabajadores con riesgos o incidencias PIE, resultado de las inspecciones realizadas.
- Contar con una herramienta informática que permita tener mayor exactitud y frecuencia en la identificación de los riesgos de protección de la información en todos los locales de los clientes del servicio PIE de la GSP.
- Brindar comunicación oportuna a los mandos del área o gerencia para tomar acciones sobre los riesgos o incidencias de Protección de la Información Empresarial identificados.

3.5.4 ALCANCE DE SISTEMA

A través del sistema de Protección de la Información Empresarial será posible:

- Realizar el registro de las incidencias producidas por los diversos trabajadores del servicio PIE de la GSP, resultado de las inspecciones in situ realizadas por los vigilantes o funcionarios de seguridad.
- Realizar el registro de las incidencias producidas por las diversas áreas del servicio PIE de la GSP, resultado de las inspecciones in situ realizadas por los vigilantes o funcionarios de seguridad.
- Realizar la autenticación de los trabajadores a través del número de inventario de la PC.
- Llevar un control exacto de los resultados de las inspecciones realizadas.
- Permitir consultar el resultado de las inspecciones a través de diversas consultas por medio de una interfase intuitiva y amigable.
- Permitir la generación automática de reportes y estadísticas de nivel gerencial.

3.5.5 EDT DE PROYECTO

En el siguiente gráfico se muestra la EDT del proyecto:

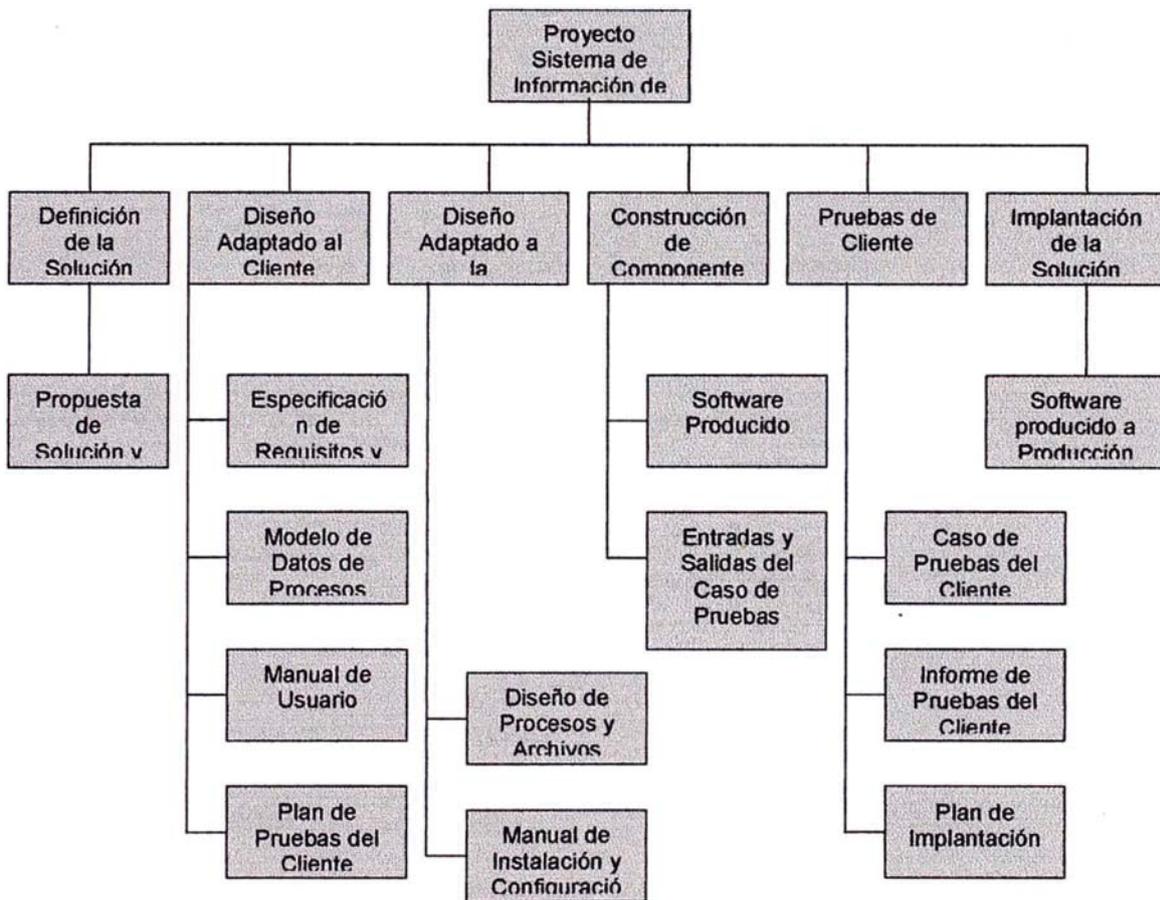


Gráfico Nº 13: EDT del Proyecto

3.5.6 DEFINICIÓN DE ENTREGABLES

Etapa MEGON	Entregables
Definición de la Solución	PR11020 - Propuesta de solución y Plan.
Diseño Adaptado al Cliente	PR21011 - Especificación de Requisitos y Diseño Externo PR11011 - Modelo de datos y procesos PR21020 - Manual de usuario PR21031 - Plan de pruebas del Cliente
Diseño Adaptado a la Construcción	PR22030: Diseño de Procesos y Archivos Físicos PR22041: Manual de Instalación y Config.
Construcción de Componentes	PR23020 - Software producido PR23031 - Entradas y salidas de casos de prueba
Pruebas del Cliente	PR81011 - Casos de pruebas de cliente PR81020 - Informe de pruebas de cliente PR81031 - Plan de implantación
Implantación de la Solución	PR82011 - Software distribuido a producción

Cuadro N° 10: Definición de Entregables

3.5.7 COSTO DE PROYECTO

Servidores: No se considera, puesto que se consideran servidores existentes en el inventario de la Empresa.

Personal: Para mayor detalle se muestra el siguiente cuadro:

Ítem	Categoría Profesional	N° horas/hombre	N° personas/categoría	Tarifa S/. (Nuevos Soles)	Precio Total S/. (Nuevos Soles)
1	Jefe de Proyecto	80	1	S/.72.50	S/. 5,800.00
2	Analista/Analista de Sistemas/Analista Funcional/Técnico de Desarrollo/Técnico de Sistemas	200	1	S/.52.50	S/. 10,500.00
3	Analista Programador/Analista Orgánico	768	1	S/.41.25	S/. 31,680.00
4	Programador	296	1	S/.31.25	S/. 9,250.00
5	Asistente Informático	96	1	S/.15.00	S/. 1,440.00
	Total servicios profesionales	1440	5		S/. 58,670.00
				Descuento por volumen:	S/. 5.000.00
				Total:	S/. 53,670.00

Cuadro N° 11: Costos del Proyecto

Licencias: Se utilizó la plataforma instalada con la que se cuenta y que tiene capacidades superiores a las recomendables, por ende no se necesitaron licencias adicionales y no son considerados como costos dentro del proyecto.

3.5.8 FASE DE ANÁLISIS Y MODELAMIENTO

3.5.8.1 MÓDULOS DE SISTEMA

- **Administración de Inspecciones:** Módulo de administración de todas las tablas y parámetros para el correcto uso del sistema. Solo acceden a este módulo los usuarios con perfil de Administrador.
- **Inspecciones:** Módulo que permite registrar las incidencias, producto de las inspecciones realizadas a los trabajadores o áreas inspeccionadas, además permite realizar consultas del resultado de las inspecciones y generar reportes de nivel gerencial para el control y la toma de acciones correctivas.
- **Histórico de Inspecciones:** Módulo que almacena la información histórica de las inspecciones realizadas, ya sea de manera automática después de "n" días (parámetro administrado en el módulo de Administración de Inspecciones) de haber finalizado la inspección o a criterio del administrador del sistema (el cual puede enviar al histórico las inspecciones en cualquier momento, con el estado de "cerrada").

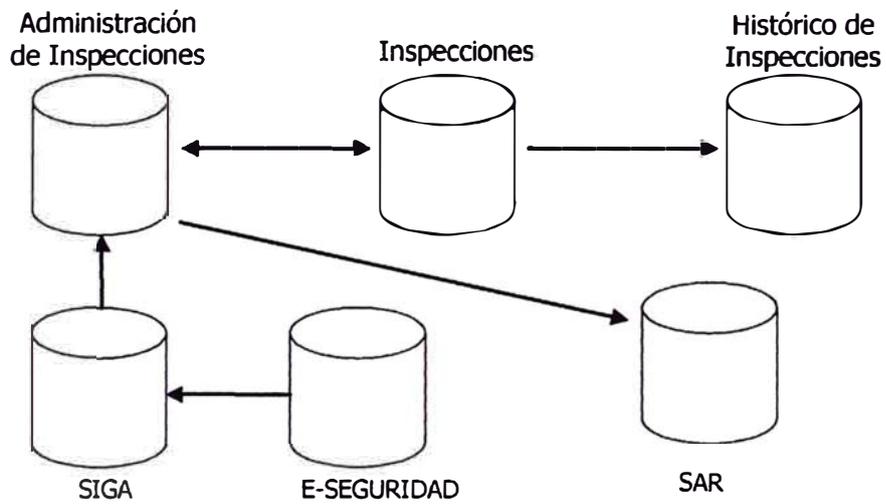


Gráfico N° 14: Módulos del Sistema

3.5.8.2 CASOS DE USO

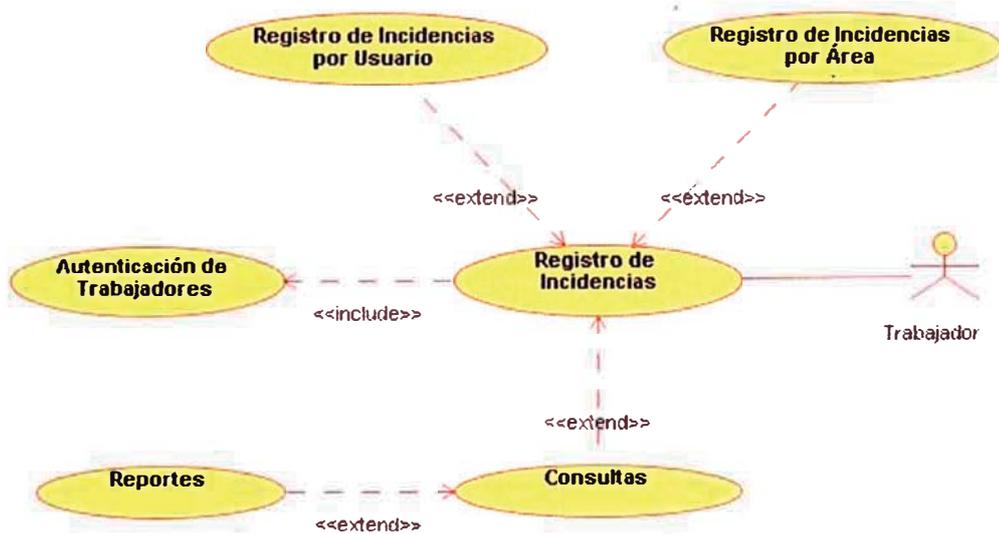


Gráfico N° 15: Diagrama de Casos de Uso del SIPIE – Incidencias

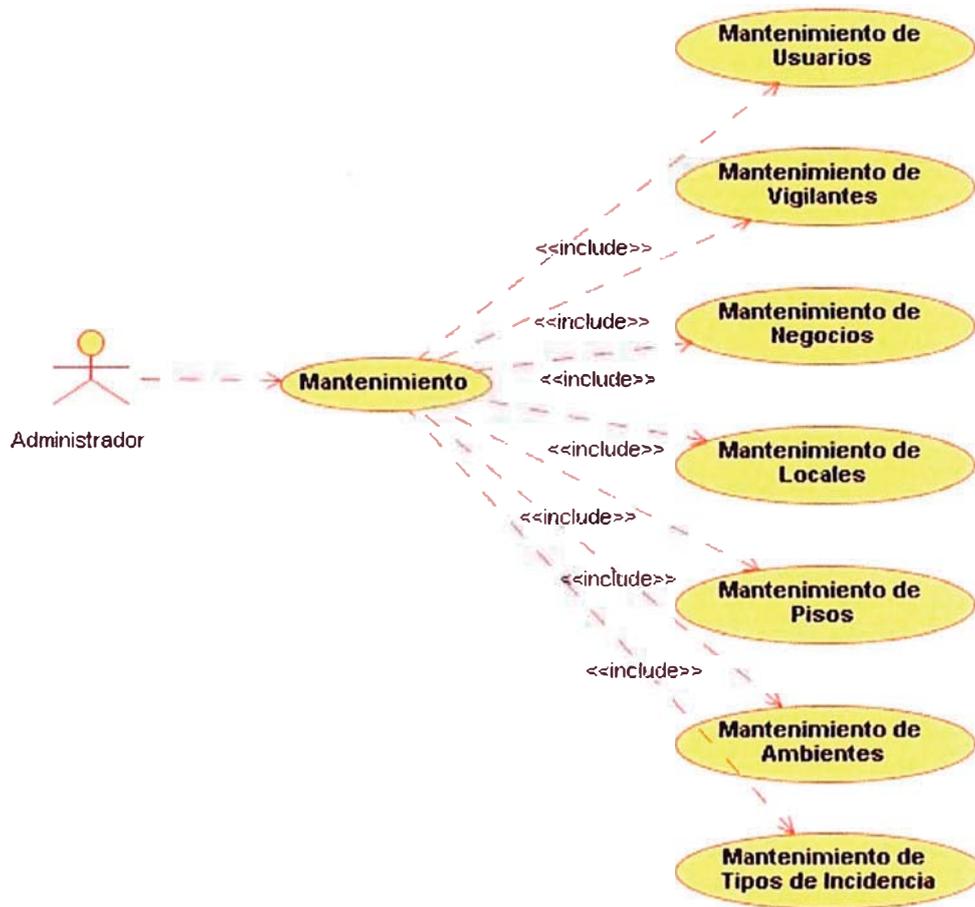


Gráfico N° 16: Diagrama UML del SIPIE – Mantenimiento

3.5.8.3 DIAGRAMA DE CLASES

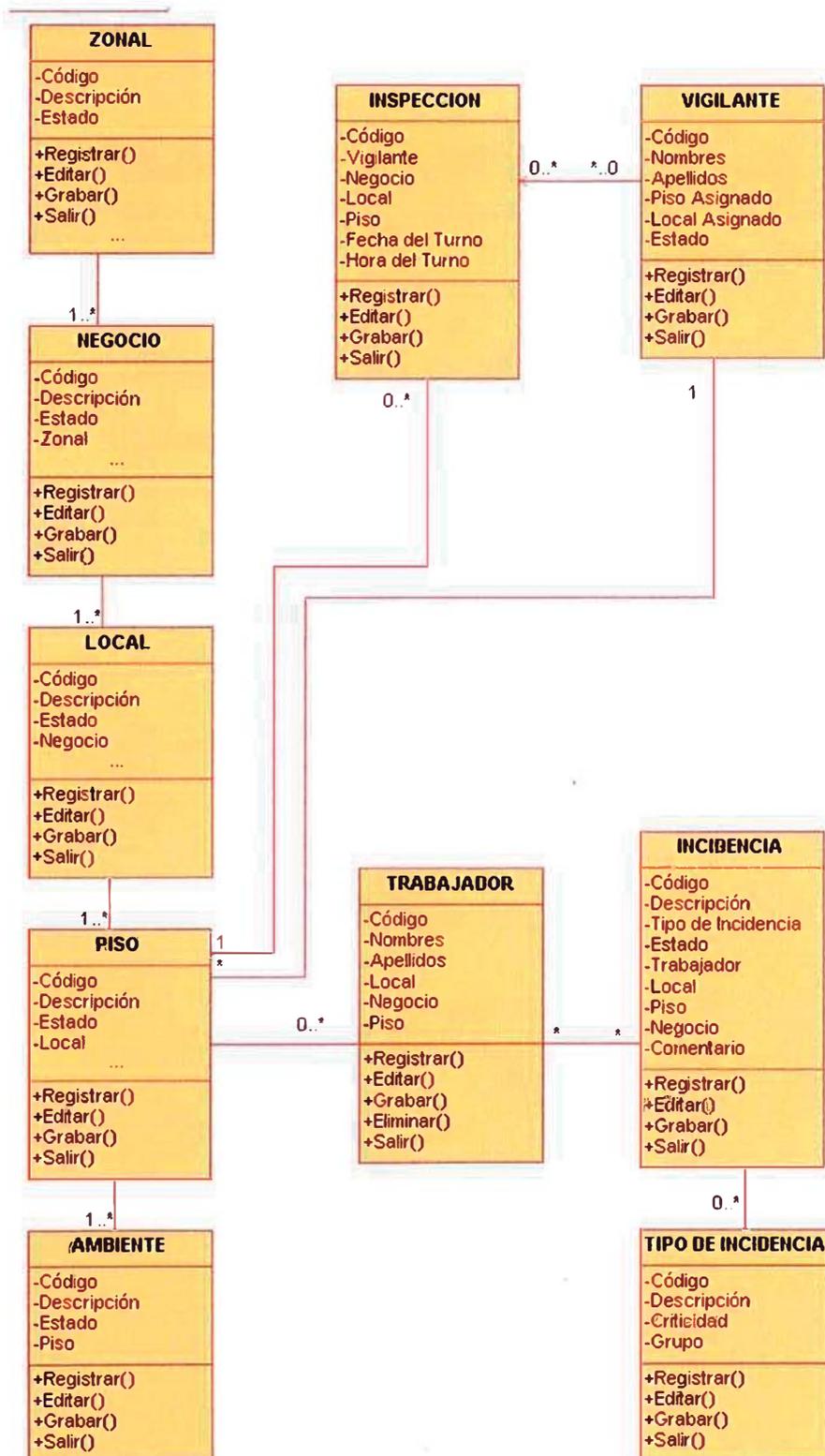


Gráfico N° 17: Diagrama de Clases del Sistema

3.5.8.4 DIAGRAMA DE ACTIVIDADES

CASO DE USO:	REGISTRO DE INCIDENCIAS
ACTORES:	Usuario (Trabajador)
TIPO	Primario
DESCRIPCION:	Permite que el usuario registre incidencias dentro de una inspección.

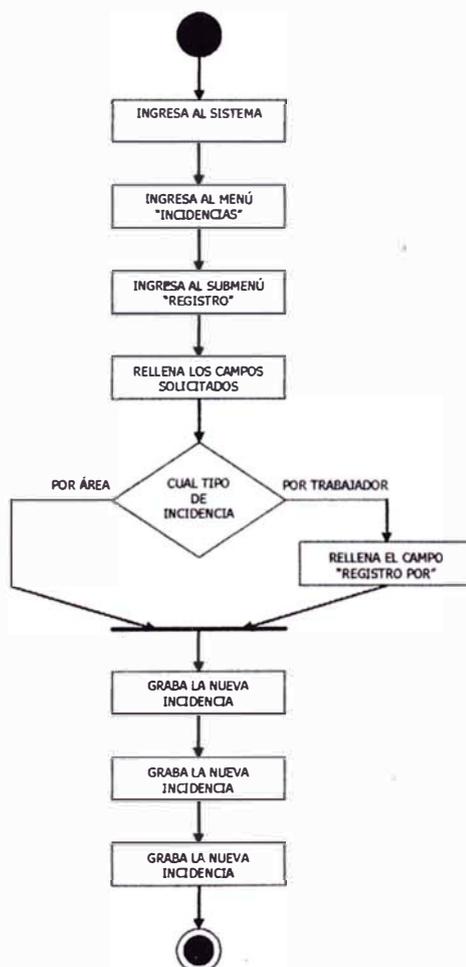


Gráfico N° 18: Diagrama de Actividades del Caso de Uso Registro de Incidencias

CASO DE USO:	AUTENTIFICACIÓN DE TRABAJADORES
ACTORES:	Usuario (Trabajador)
TIPO	Primario
DESCRIPCION:	Permite que el usuario pueda acceder al sistema.

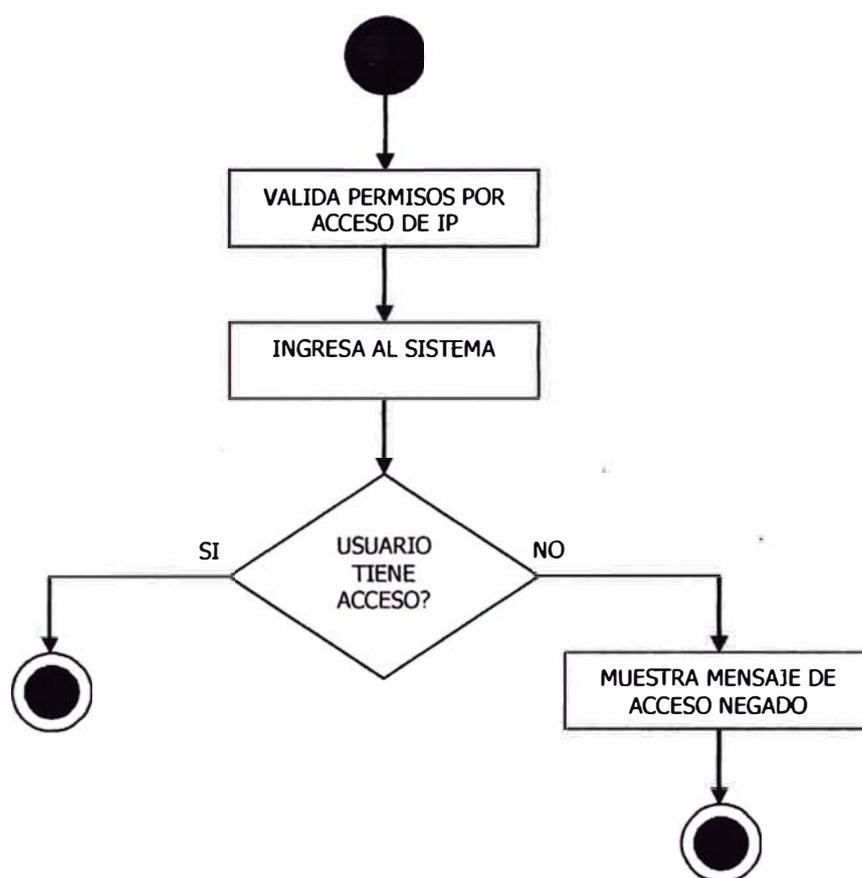


Gráfico N° 19: Diagrama de Actividades del Caso de Uso Autenticación de Trabajadores

CASO DE USO:	REPORTES
ACTORES:	Usuario (Trabajador)
TIPO	Primario
DESCRIPCION:	Permite generar reportes de interés.



Gráfico N° 20: Diagrama de Actividades del Caso de Uso Reportes

CASO DE USO:	CONSULTAS
ACTORES:	Usuario (Trabajador)
TIPO	Primario
DESCRIPCION:	Permite realizar consultas de incidencias.

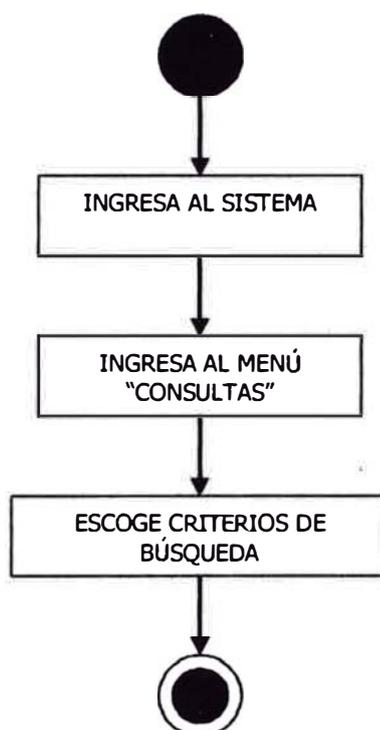


Gráfico N° 21: Diagrama de Actividades del Caso de Uso Consultas

USUARIOS DEL SISTEMA

Ejecutor: Sólo puede ingresar información. (Personal de Seguridad - Vigilancia)

Consulta: Sólo puede consultar información. (Personal de GSP)

Operador: Puede ingresar y consultar información. (Personal de Seguridad, Personal de la GSP)

Administrador: Tiene acceso a modificación de tablas generales como: Locales, Trabajadores, Ambientes, etc.

3.5.9 FASE DE DISEÑO

3.5.9.1 PROTOTIPOS DEL SISTEMA

Administración del Sistema: Para ingresar desde el área de trabajo Notes se debe dar doble clic al siguiente icono:



El menú principal de Administración es el siguiente:

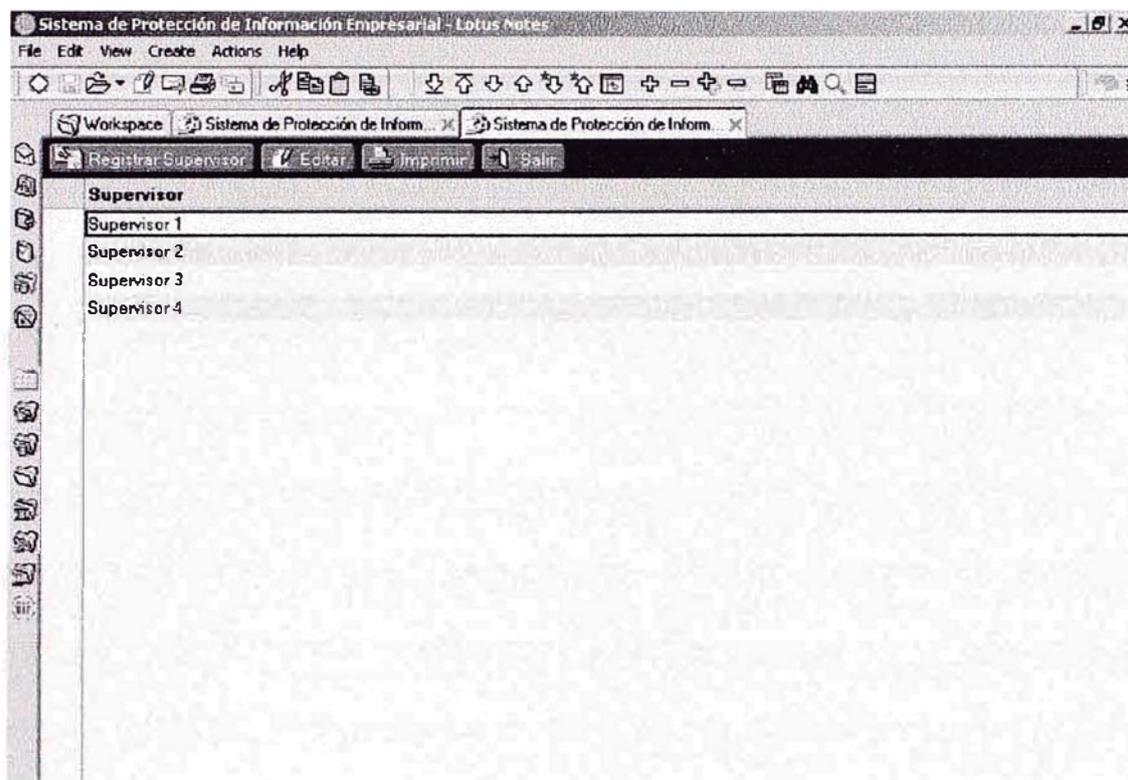


Gráfico N° 22: Pantalla Principal del Módulo de Administración

Tipos de Incidencia: Para registrar y actualizar la información de los tipos de Incidencia se debe dar clic en “Tipos de Incidencia”, aparecerá la relación de los tipos de incidencias registrados:

Código	Descripción
▼ Area	
A01	Documentos expuestos en fotocopiadoras.
A02	Documentos expuestos en impresoras del área
A03	Amarrios abiertos o cerrados sin llave
A04	Archivadores gaveteros abiertos o cerrados sin llave
▼ Trabajador	
T01	Documentos expuestos (incluye impresora personal)
T02	Diskettes o CD's expuestos
T03	Cajones abiertos o cerrados sin llave
T04	Documentos destruidos inadecuadamente en el tacho
T05	Archivadores de palanca (con documentos) expuestos
T06	Computadora prendida y sin bloquear

Supervisores: Para registrar y actualizar la información de los Supervisores se debe dar clic en "Supervisores" desde el menú de administración:



Usuarios x PC: Para registrar y actualizar la información de los Usuarios por PC, se debe dar clic en “Usuarios x PC” desde el menú de administración. Al ingresar a la opción el sistema muestra la relación de los usuarios por PC agrupados por Negocios.

Local	Nombres	Apellidos	Nro Inventario	Anexo
Surquillo	Usuario 1		4512	110
Surquillo	Usuario 2			113
Surquillo	Usuario 3		4513	
Surquillo	Usuario 5		4515	112

Protección de la Información Empresarial: Para ingresar desde el área de trabajo Notes se debe dar doble clic k al siguiente icono:

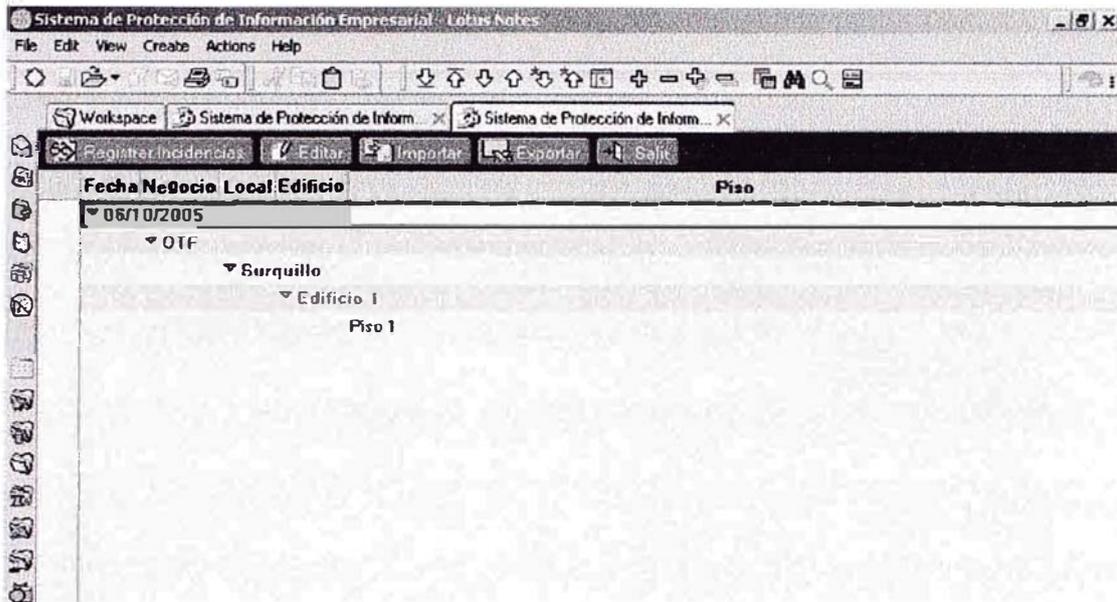


Aparece el menú principal de Protección de la Información mostrado anteriormente, esta vez seleccionamos "Registro" (aparece un menú como el que se muestra a continuación):

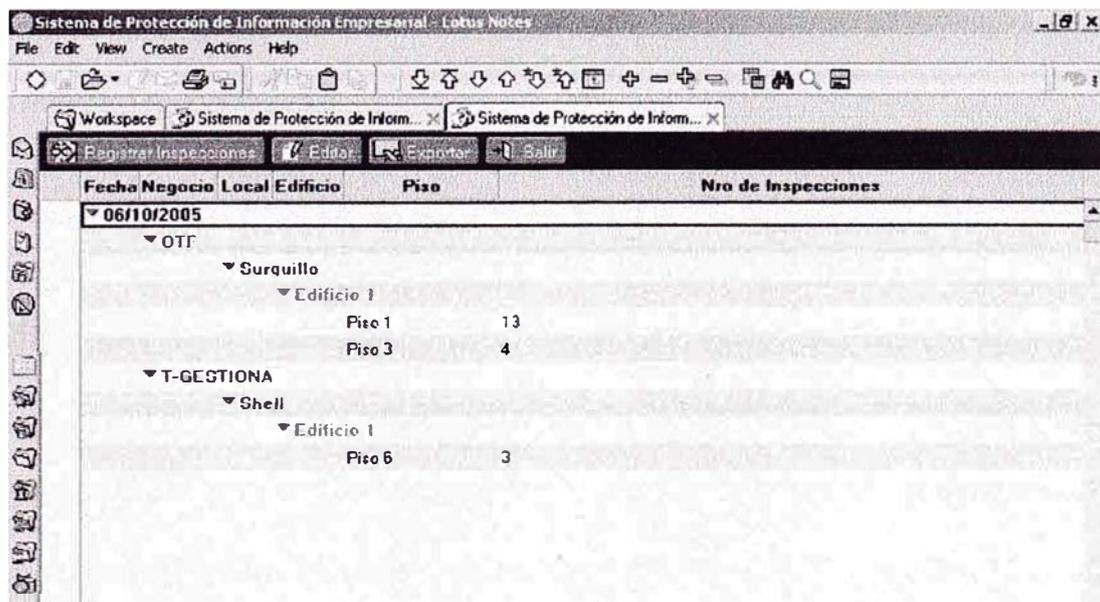


Gráfico N° 23: Pantalla Principal del Sistema

Incidencias: Desde el Menú de registro se debe seleccionar la opción "Incidencias" la cual muestra la siguiente vista con la relación de las incidencias registrada:



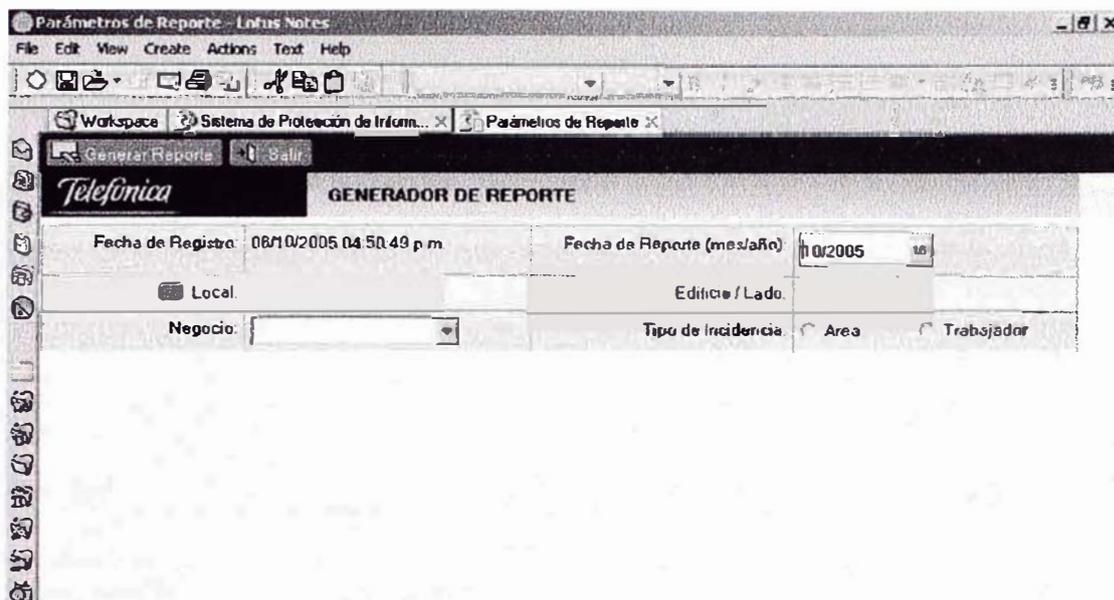
Inspecciones: Desde el menú de registro se debe seleccionar la opción “Inspecciones” el cual muestra el siguiente formulario para el registro de todas las inspecciones realizadas en el día:



Consultas: Luego de dar click en “Consultas” aparece un menú como el que se muestra a continuación:



Reportes: Luego de dar click en “Reportes” aparece un formulario como el que se muestra a continuación:



Al realizar filtros de generación de reportes, y después presionar el botón “Generar Reporte”:

Usuario						
A	B	C	D	E	F	
1	Usuario	Daniel Pruebas		Local		
2	Fecha de Em.	06/10/2005 - 17:25:25		Mes de Reporte		
3						
4						
5	N°	FECHA	PISO	IDENTIFIC	Documentos expuestos	Documentos expuestos en impres
6	1	10/08/2005	Piso 1		1	1
7	2	10/05/2005	Piso 4		1	1
8	3	10/03/2005	Piso 4		1	0
9	4	10/04/2005	Piso 4		0	1
10	5	10/02/2005	Piso 4		0	1
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						

3.5.9.2 DISEÑO EXTERNO DEL SISTEMA

Ingreso del Usuario al Sistema: Se realiza a través de la validación del usuario y clave de acceso, siguiendo las políticas de seguridad de la empresa.

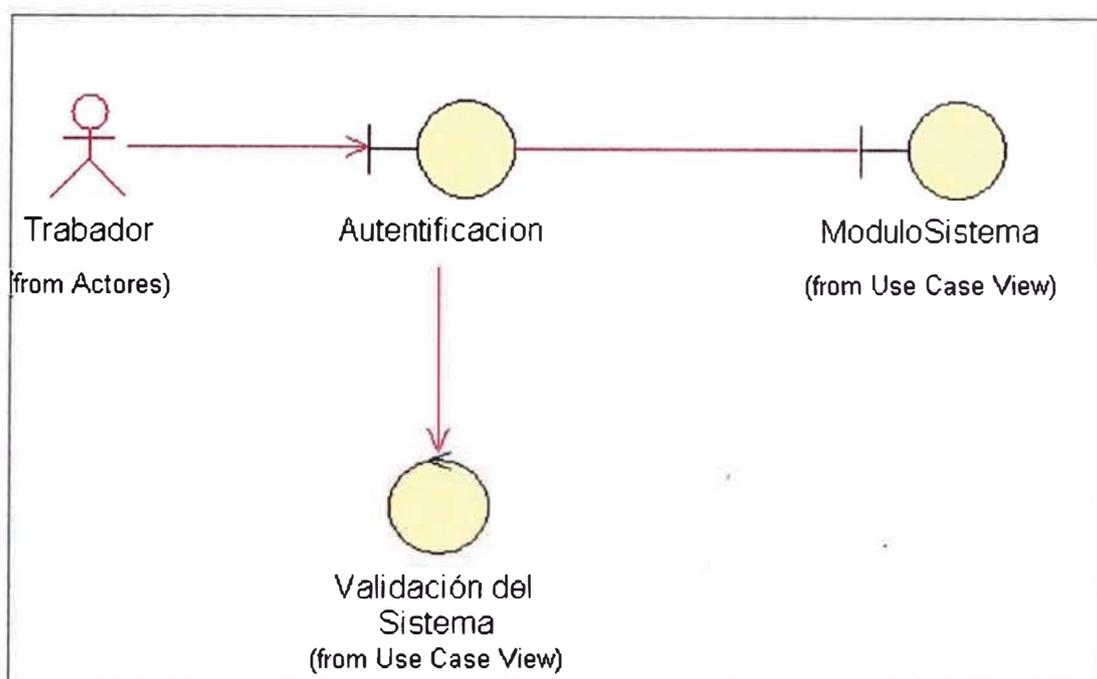


Gráfico N° 24: Diagrama UML del Ingreso del Usuario

Administración del Sistema: Se realiza a través del módulo de Administración de Inspecciones, el cual administra todas las tablas y parámetros que facilitan el uso del sistema y ayudan a dar frente a los cambios que se produzcan en la empresa.

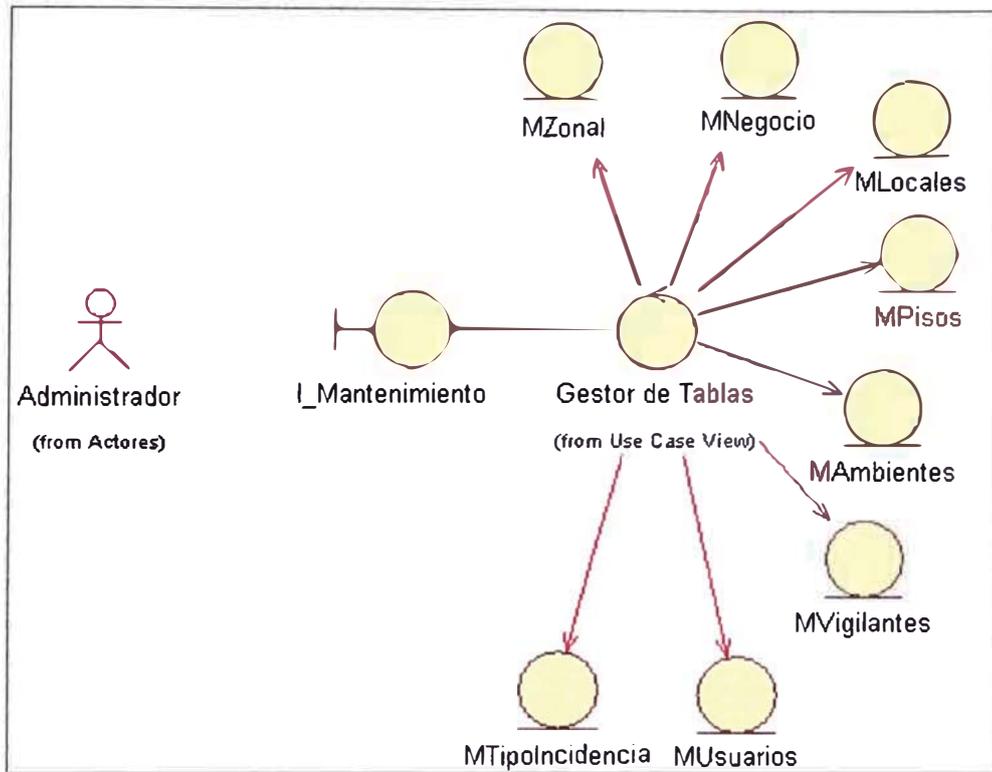


Gráfico N° 25: Diagrama UML de la Administración del Sistema

Registro de Incidencias del Empleado: Permite registrar las incidencias producidas por los empleados incluidos en una cierta inspección.

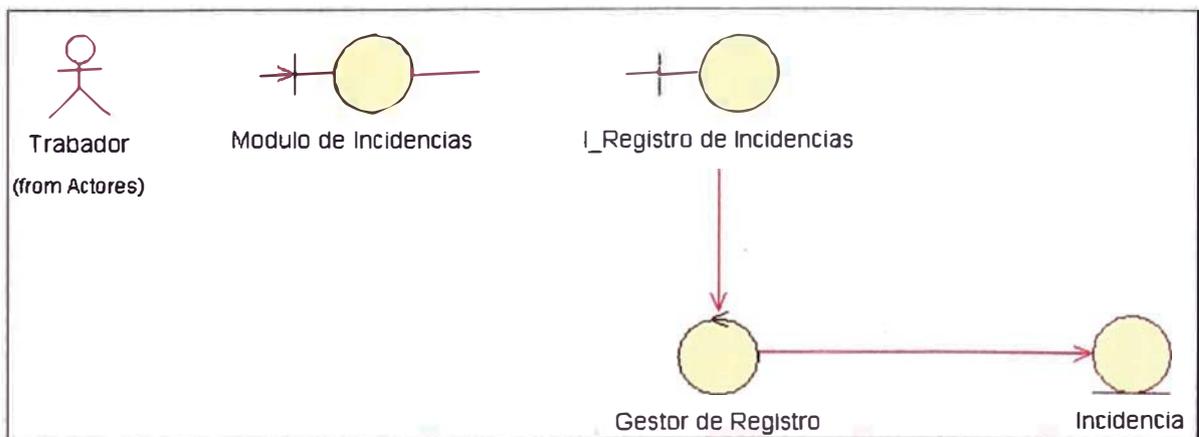


Gráfico N° 26: Diagrama UML del Registro de Incidencias

Consultas: Permite visualizar a través de vistas las incidencias registradas en el sistema de acuerdo a diversos criterios (Vigilante, Número de Inventario de PC, Área, Estado de Inspección, Zonal, Negocio, Local, Piso, Fecha, Tipo de Incidencia)

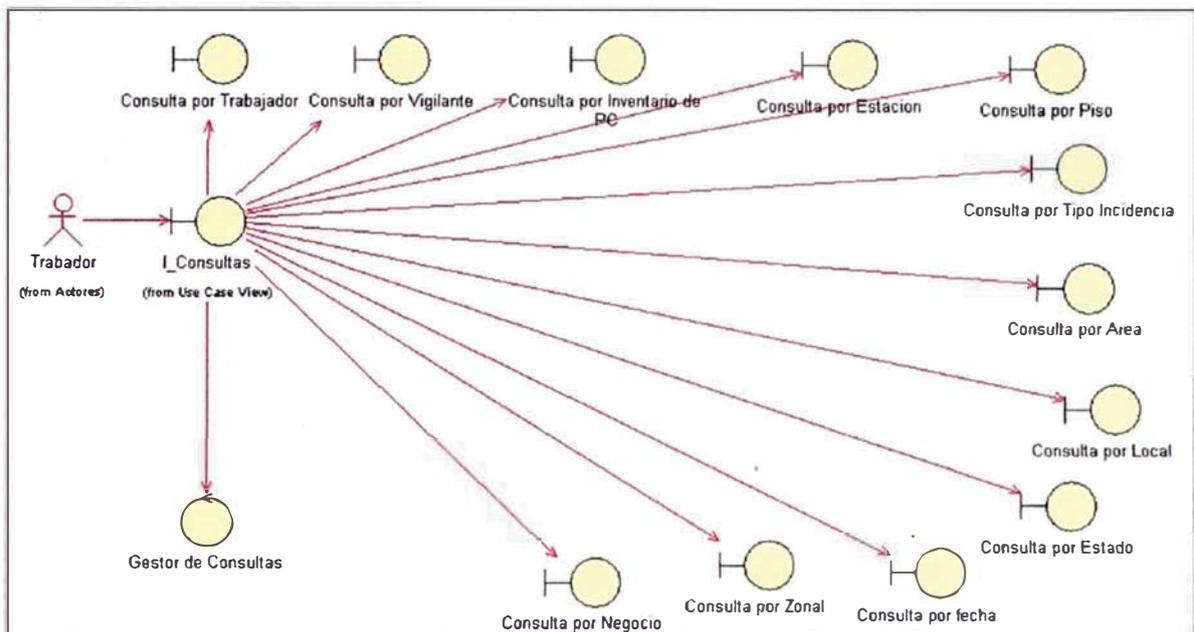


Gráfico Nº 27: Diagrama UML de Consultas

Reportes y Estadísticas: Los usuarios autorizados generan de manera automática reportes y estadísticas de nivel gerencial en Excel y definidas de acuerdo a un rango de fechas establecido por el usuario al momento de solicitar el reporte.

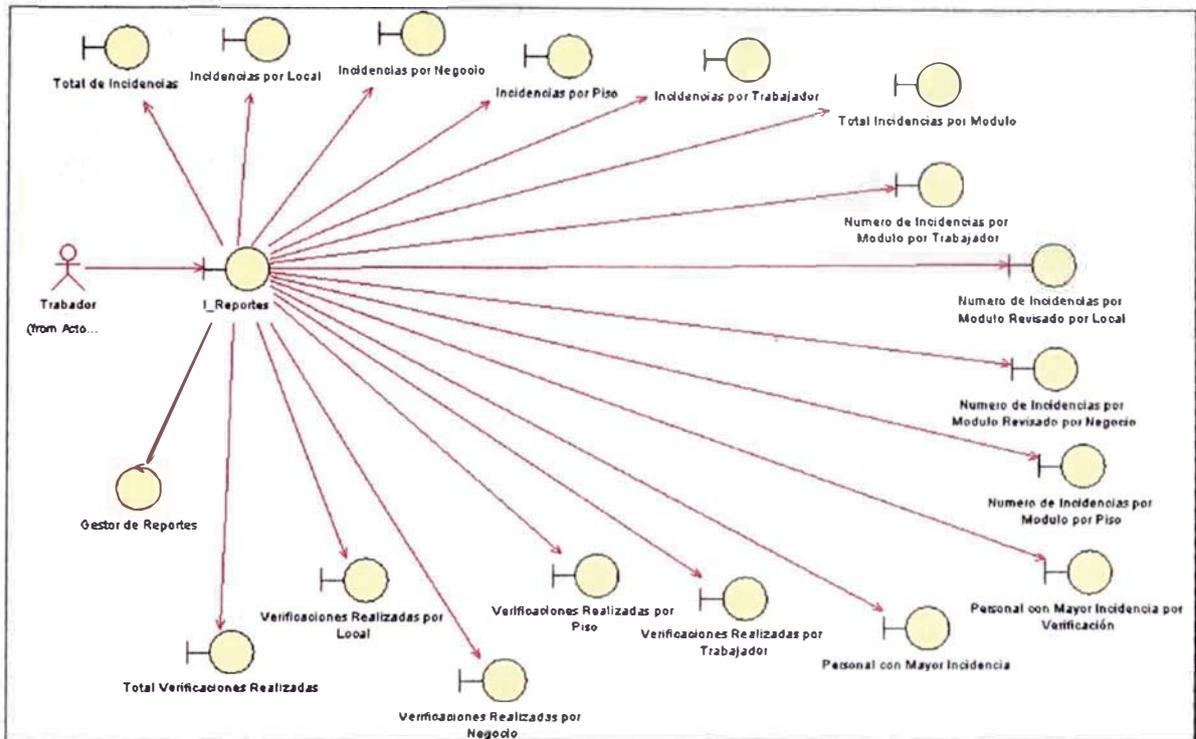


Gráfico N° 28: Diagrama UML de los Reportes y Estadísticas

Histórico del Sistema:

En este módulo se almacenan las inspecciones con estado "Cerrada".

3.5.10 DISEÑO DE ARCHIVOS FÍSICOS

3.5.10.1 DIAGRAMA DE BASES DE DATOS

El SIPIE se encontrará compuesto de las siguientes bases de datos documentales:

- Administración del Sistema
- Protección de la Información
- Inventario SIGA (Base de datos de apoyo del Sistema de Gestión Administrativa SIGA)

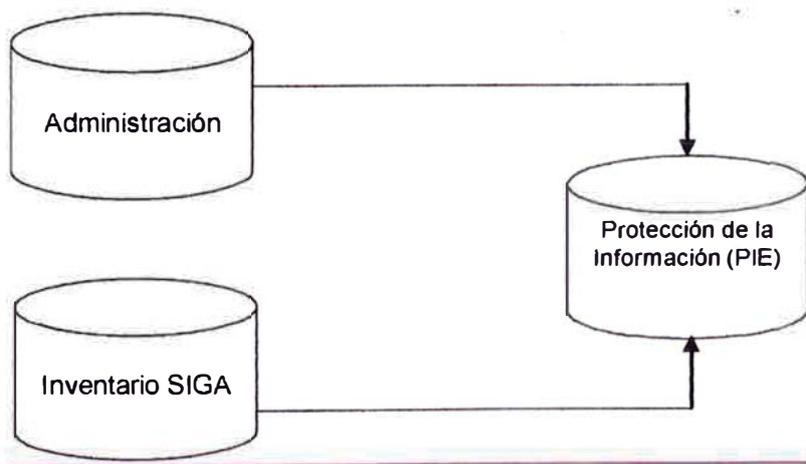


Gráfico N° 29: Diagrama de Bases de Datos SIPIE

3.5.10 DISEÑO DE ARCHIVOS FÍSICOS

3.5.10.1 DIAGRAMA DE BASES DE DATOS

El SIPIE se encontrará compuesto de las siguientes bases de datos documentales:

- Administración del Sistema
- Protección de la Información
- Inventario SIGA (Base de datos de apoyo del Sistema de Gestión Administrativa SIGA)

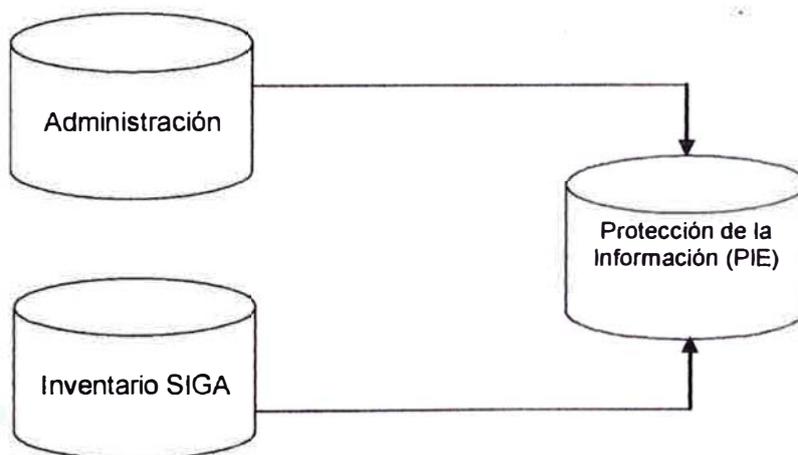


Gráfico N° 29: Diagrama de Bases de Datos SIPIE

3.5.10.2 MODELO DE DATOS

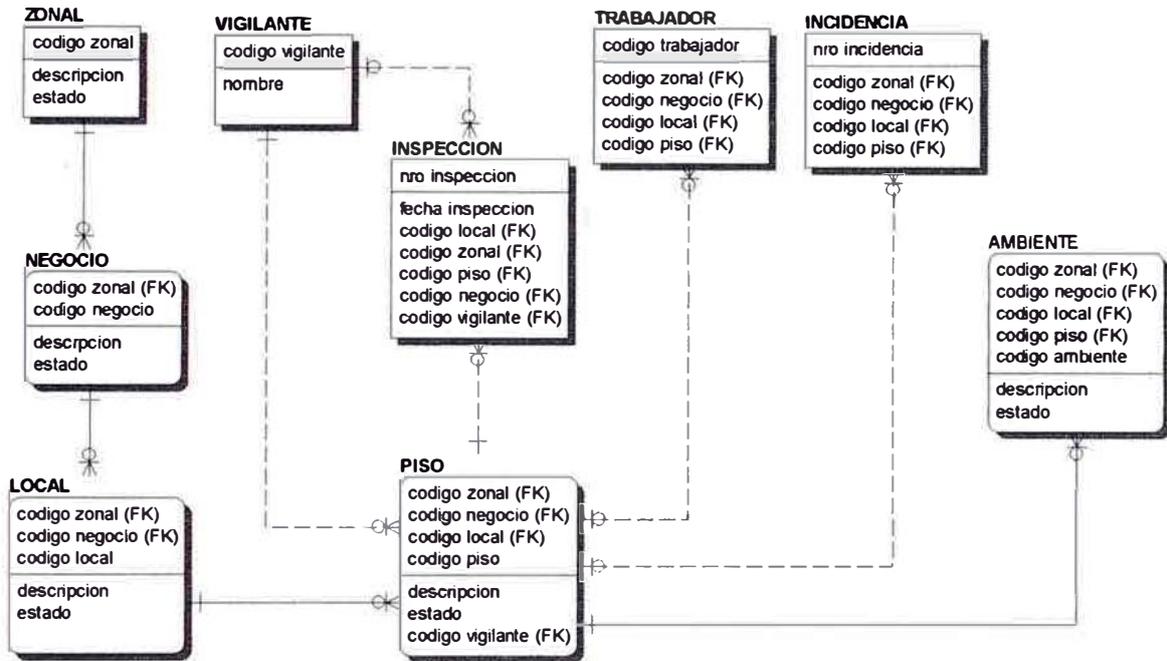


Gráfico N° 30: Diagrama Lógico de Datos SIPIE

Las entidades que intervienen en el sistema son las siguientes:

Nombre Físico de Entidad	Descripción de la Entidad
Zonal	Entidad donde se administran las diversas zonales en las cuales se realiza las inspecciones.
Negocio	Entidad donde se administran los diversos negocios por zonal en donde se realizan las inspecciones.

Local	Entidad donde se administran los diversos locales por negocio en donde se realizan las inspecciones.
Piso	Entidad donde se administran los diversos pisos por local en donde se realizan las inspecciones.
Ambiente	Entidad donde se administran los diversos ambientes por piso en donde se realizan las inspecciones.
Vigilante	Persona autorizada para realizar la inspección, el cual contendrá las incidencias detectadas.
Inspección	Detalle de la inspección realizada, contiene el detalle de las incidencias registradas.
Incidencia	Entidad donde se administran las diversas incidencias encontradas en las inspecciones.
Tipo de Incidencia	Entidad donde se administran los diversos tipos que puede clasificarse una incidencia.
Trabajador	Usuario involucrado en una incidencia registrada.

A) Base de Datos Administración

Contiene todos los parámetros del sistema, los cuales deberán ser configurados por el Administrador del Sistema.

Relación de Formularios:

Supervisores:

Nº	Nombre	Tipo
1	Supervisor	Nombres

Tipos Incidencia:

Nº	Nombre	Tipo
1	CodigoIncidencia	Texto
2	DescripcionIncidencia	Texto
3	TipoIncidencia	Botones Radiales

Usuarios x PC:

Nº	Nombre	Tipo
1	Nombres	Texto
2	Apellidos	Texto
3	Local	Texto
4	Negocio	Combo
5	NumeroInventario	Texto
6	NumeroAnexo	Texto
7	FechaRegistro	Fecha

Relación de Vistas:

- Tipos Incidencia
- Usuarios x PC

B) Base de Datos Protección de la Información

Contiene información de las incidencias e inspecciones registradas.

Relación de Formularios:

Documento Resumen:

Nº	Nombre	Tipo
1	FechaRegistro	Fecha
2	FechaInspeccion	Texto
3	Local	Texto
4	Edificio	Texto
5	Negocios	Texto
6	Piso_1	Lista Texto
7	Inspeccion_1	Lista Texto
8	Incidencia_1	Lista Texto
9	Porcentaje_1	Lista Texto
10	Incidencia	Lista Texto
11	Piso_2	Lista Texto
12	Inspeccion_2	Lista Texto
13	Incidencia_2	Lista Texto
14	Porcentaje_2	Lista Texto

Incidencias:

N°	Nombre	Tipo
1	Codigo	Texto
2	Tipoincidencia	Botones Radiales
3	Estado	Texto
4	UsuarioLotus	Texto
5	Vigilante	Texto
6	Local	Texto
7	Edificio	Texto
8	Piso	Texto
9	Negocio	Combo
10	TipoRegistro	Botones Radiales
11	NumeroInventario	Texto
12	NumeroAnexo	Texto
13	NombreTrabajador	Nombres
14	Incidencias	Casillas
15	dsplIncidencias	Texto
16	Comentarios	Texto Enriquecido
17	Anexos	Texto Enriquecido

Inspecciones:

N°	Nombre	Tipo
1	FechaRegistro	Fecha
2	Vigilante	Texto
3	Local	Texto
4	Edificio	Texto
5	Piso	Texto

6	Negocio	Combo
7	FechaInspeccion	Fecha
8	NroInspecciones	Número
9	Comentarios	Texto Enriquecido
10	Anexos	Texto Enriquecido

Reportes:

Nº	Nombre	Tipo
1	FechaRegistro	Fecha
7	FechaInspeccion	Fecha
3	Local	Texto
4	Edificio	Texto
5	TipoIncidencia	Botones Radiales
6	Negocio	Combo
5	Piso	Texto

Relación de Vistas:

- Consulta\Por Anexo
- Consulta\Por Estado
- Consulta\Por Fecha
- Consulta\Por Local
- Consulta\Por Negocio
- Consulta\Por Tipo Incidencia
- Consulta\Por Vigilante
- Inspecciones\Por Fecha

C) Base de Datos de Inventario (SIGA)

Esta base de datos pertenece al sistema SIGA. De esta base de datos se extrae información acerca los edificios, pisos, locales, negocios relacionados, etc.

3.5.11 FASE DE PRUEBAS (TESTING)

El objetivo de esta fase es confirmar que la funcionalidad requerida y desarrollada está funcionando de manera adecuada.

La estrategia utilizada para realizar las pruebas del sistema consistió en:

- Definir los distintos perfiles de los usuarios clientes del sistema así como los distintos procesos que realizan dentro del sistema.
- Planificar las pruebas de acuerdo a los distintos perfiles.
- Se planificaron las pruebas de acuerdo a la importancia de los procesos.
- La planificación involucrará pruebas durante las mañanas y ajuste sobre los programas en las tardes (incidencias), la mañana siguiente deberá volverse a probar para confirmar que todo está corregido.
- Se consideró un recurso desarrollador adicional quien realizó la segunda y tercera prueba con el usuario, esto sin alterar las pruebas siguientes planificadas.

Se dio por finalizadas las pruebas (basadas en un El plan de pruebas) cuando se pueda concluir que los ajustes necesarios son menores y no impiden el flujo del sistema o no afectan una funcionalidad importante o que no afecte a otros procesos importantes. En total tomó 10 días las pruebas.

Para la planificación de las pruebas se consideró los siguientes perfiles:

CÓDIGO	DESCRIPCIÓN
001	SUPERVISOR
002	ADMINISTRADOR

Cuadro N° 12: Perfiles de Usuario del Sistema

3.5.12 FASE DE IMPLEMENTACIÓN

3.5.12.1 CENTROS DE IMPLANTACIÓN

1. En el Servidor Domino: El sistema fue instalado en un servidor Domino de producción (el cual centraliza la información relativa a las bases de datos).
2. En las estaciones de trabajo de los usuarios: Es necesario que cuenten con el Lotus Notes Desktop instalado y la configuración de los iconos de la aplicación en el escritorio de Notes, por ende se envió un mensaje de correo con la ruta ("Link") la misma que al ser ejecutado (con doble clic) se quedará fijado.

3. En las estaciones de trabajo de los usuarios Administradores: Instalación de los iconos en el escritorio (Desktop Notes) de los usuarios Administradores, para lo cual se envió un mensaje de correo con la ruta ("Link") la misma que al ser ejecutado (con doble clic) se quedará fijado. (Idéntico al ítem anterior)

3.5.12.2 ARQUITECTURA DEL SISTEMA

La arquitectura del presente sistema debe constar de: (requerimientos para la implementación)

- **Arquitectura:**

Lotus Domino Server R5, R6

Sistemas Operativos: Windows NT (Intel), AIX (RS/6000), OS/400 (AS/400), OS/390 (S/390), OS/2, Red Hat Linux, Solaris.

- **Hardware:**

Plataforma: Compaq

Servidor: Lotus Domino - SDELCLI104

Procesador del Servidor: Pentium IV 1.0 Ghz. o superior

Capacidad del Servidor: 15 GB mínimo de espacio en disco - 1024 Mb RAM

Sistema Operativo: Windows 2000

Base de Datos: Lotus Notes Desktop R5

- Software:

Lenguaje de Programación: Lotus Domino - Designer

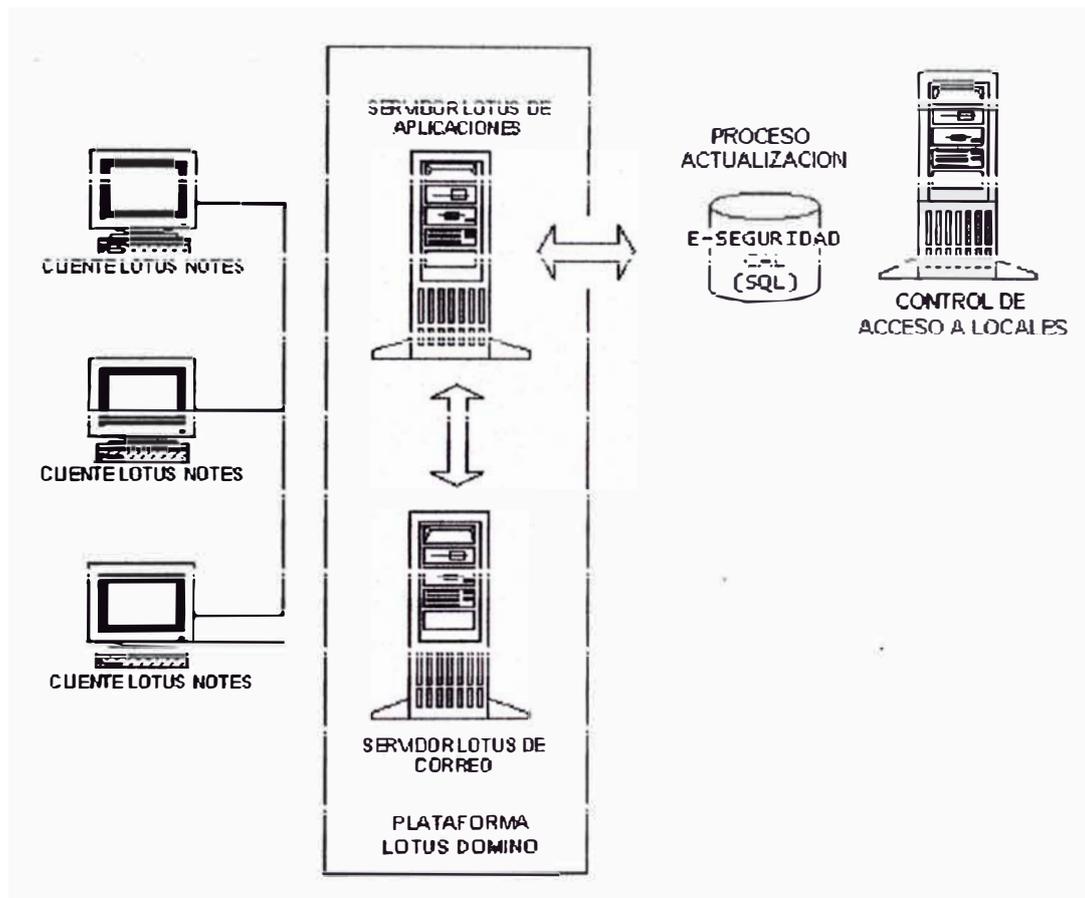


Gráfico N° 31: Arquitectura del Sistema

3.5.12.3 ESTRATEGIA DE IMPLEMENTACIÓN

El despliegue del sistema SIPIE a los usuarios involucrados se dio mediante un correo, el cual contenía los enlaces (link) de las bases de datos correspondientes al sistema.

3.5.12.4 PLANIFICACIÓN

- Puesta en producción de las bases de datos, en servidor y clientes.
- Definición de los usuarios administradores, encargados de llenar las tablas administrativas necesarias.
- Ingreso de parámetros de configuración (ubicación de bases de datos).
- Definición de los usuarios, cargos y roles asignados por los usuarios administradores.
- Carga de usuarios, cargos y roles por los usuarios administradores.
- Entrenamiento de los usuarios involucrados.

CAPÍTULO 4

EVALUACIÓN DE RESULTADOS

La evaluación de los resultados está orientada a cubrir las necesidades y dar solución a los problemas planteados en el informe. Los resultados obtenidos del uso del sistema implementado han sido excelentes, inclusive han sobrepasado los objetivos planteados.

Algunos de ellos son:

- Mayor compromiso de las diversas áreas con la PIE: Al tener informes en tiempo real y fidedignos, se han tomado medidas para que las incidencias sean reducidas en su frecuencia, lo cual ha hecho que los empleados lo tomen en cuenta en sus labores diarias.
- Menor frecuencia de incidencias: Agregando a lo mencionado en el ítem anterior, la frecuencia de las incidencias se ha reducido en un 20%, lo cual es un buen índice, sin embargo todavía queda pendiente una mayor reducción.

- Mayor rapidez de generación de reportes: Con el sistema ya implementado, el equipo PIE de la GSP demora solo 4 horas laborales en generar el reporte. Antes del sistema, se demoraba 40 horas para generar estos reportes.
- Estandarización de Reportes: Además de la mayor rapidez de generación, ahora se cuenta con un solo tipo (plantilla) de reporte, lo cual optimiza el procesamiento de la información por parte de la GSP y los distintos estamentos de la empresa.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- Se logró contar con un único repositorio de información en el cual se almacenen todos los registros de inspecciones, eliminado el uso de carpetas compartidas y evitando que la información se encuentre expuesta a virus o robos informáticos.
- Se contribuyó a que los empleados tuvieran muy en cuenta proteger la información confidencial de la empresa, con medidas tomadas en base a los informes generados, esto permitió reducir la frecuencia de las incidencias en un 20%.
- Se logró estandarizar para todos los locales el formato de registro de inspecciones realizadas por el personal de vigilancia, facilitando de esta manera su consolidación y posterior análisis.

- Se mejoró el proceso de identificación de los trabajadores con riesgos PIE, por consecuencia se agilizó la entrega de los reportes a los mandos del área o gerencia, tomando en promedio medio día de atraso luego de ser finalizadas las inspecciones.

RECOMENDACIONES

- Almacenar y actualizar en el sistema SAR el número de inventario de PC del usuario. Existirá un proceso que actualizará en el sistema SAR el número de inventario de PC y el nombre de la PC del usuario.
- Desarrollar la funcionalidad de calendarizar el registro de inspecciones, mediante el cual los vigilantes encargados de registrar inspecciones podrán establecer un cronograma de todas las inspecciones que deben realizar dentro de un rango de fechas determinado, éste registro será almacenado en la agenda de Lotus Notes de cada uno de los usuarios, de tal manera que cuando se aproxime la fecha de realizar la inspección el sistema de manera automática enviará una notificación vía correo electrónico a los responsables indicando la proximidad de la inspección. Así podrán generar cronogramas para ordenar su trabajo.

GLOSARIO DE TÉRMINOS

Incidencia: Todo suceso que atenta contra la seguridad de información de una empresa.

ISO 17799: Guía para la implementación de un sistema de administración de la seguridad de la información, preserva los principios de confidencialidad, integridad y disponibilidad.

MEGON: Marco Estratégico de Gestión Orientada al Negocio.

PIE: Protección de la Información Empresarial.

Pulso: Unidad de medición de las llamadas telefónicas.

Seguridad Informática: Estado de cualquier sistema informático que nos indica que el sistema está libre de peligro, daño o riesgo (al menos en un % considerable).

Seguridad de la Información: Protege la información confidencial de una empresa, definiendo estrategias efectivas que garanticen una gestión segura de los procesos del negocio a fin de darle mayor resguardo a la información.

BIBLIOGRAFÍA

- **Análisis y Diseño Orientado a Objetos con UML y Rational Rose – Sergio Matsukawa**
- **Apuntes del Curso de Análisis y Diseño de Sistemas del Ing, Luis Zuloaga Rotta.**
- **Apuntes del Curso de Auditoría de Sistemas del Ing. Carlos Trigo.**
- **Manual de Lotus Notes – IBM**
- **Metodología MEGON - Telefónica**

ANEXOS

Anexo 1: Pilares Fundamentales de la Visión del Grupo



Gráfico N° 32: Pilares para la Visión del Grupo

A) ORIENTACIÓN AL CLIENTE

La estrategia de la compañía consiste en crear un Grupo dotado de una visión orientada al cliente uniforme y coherente. Teniendo en cuenta que, actualmente, el cliente es un cliente "multiservicio", La empresa es consciente de la necesidad de posicionarse con una visión integral y uniforme que comprenda la oferta

comercial de una serie de soluciones demandadas por el cliente y propuestas por el Grupo.

De esta forma, el Grupo se ha convertido en un referente mundial, con una orientación estratégica claramente definida hacia un servicio al cliente más personalizado, la diferenciación de soluciones para las diferentes necesidades y la segmentación de clientes en cuatro grandes grupos: individuales, familias, PYMES y grandes empresas y administraciones públicas.

Diferentes compañías pertenecientes al Grupo han lanzado programas de transformación interna para alcanzar estos objetivos; son casos representativos los del Grupo de España con el programa "meta:cliente", Telefónica Internacional con "Compromiso Cliente". Telefónica Móviles está ejecutando programas orientados a "Resolución al primer contacto" y "Renovación del Sistema Comercial", entre otros.



Gráfico N° 33: Acelerar para ser más líderes: orientación al cliente

El Grupo pretende crecer incrementando su base de clientes actual con ofertas innovadoras y a la medida de cualquier tipo de cliente.

Además, espera integrar totalmente el conjunto de la sociedad en el mundo de las telecomunicaciones y está realizando inversiones para la democratización del sector, poniéndose como objetivo la oferta de sus servicios a segmentos del mercado que actualmente tienen dificultades para acceder a este sector.

Responden a esta filosofía los modelos de facturación adaptados a clientes de escasos recursos, los servicios innovadores para discapacitados y los servicios de valor añadido para pequeñas y medianas empresas.

En el siguiente gráfico se muestran los principios fundamentales del Grupo para relacionarse con eficiencia y eficacia con los clientes:

Número	Principio	Explicación
1	Conocimiento	En el Grupo Telefónica, queremos entender a nuestros clientes, lo que necesitan y desean, esforzándonos en escucharlos para conocer, comprender y satisfacer sus inquietudes y necesidades.
2	Innovación	Llegar donde los demás no llegan, innovar en lo que hacemos y en cómo lo hacemos es ofrecer a nuestros clientes productos y servicios que hagan su vida más fácil.
3	Calidad	Trabajamos para ganarnos la confianza de nuestros clientes esforzándonos cada día en conseguir la máxima calidad en nuestras actividades y la de nuestros colaboradores, en nuestros productos, en nuestros servicios y en nuestro trabajo diario.
4	Personalización	En el Grupo Telefónica trabajamos para Juan, María y Ángela... personas, no números, hombres y mujeres con necesidades y aspiraciones que tenemos que atender en todo el mundo, como ellos quieren.
5	Compromiso de todos	Todos formamos parte del Grupo Telefónica y todos, en cada puesto, en cada departamento, trabajamos para mantener y fortalecer la relación de Telefónica con nuestros clientes a largo plazo.
6	Transparencia	Queremos mantener con nuestros clientes comunicaciones transparentes y sinceras, facilitándoles, como Grupo integrado, la resolución de sus dudas e inquietudes.
7	Garantía de Satisfacción	Reconocer nuestros fallos y ofrecer a nuestros clientes la solución adecuada, nos garantiza plenamente su satisfacción en el tiempo.

Gráfico N° 34: Principios de la relación del Grupo con el cliente

B) INNOVACIÓN

El Grupo concibe la Innovación como uno de los pilares en los que se asienta su transformación y dedica plenamente el esfuerzo de sus empleados a la innovación tecnológica, comercial y de procesos.

C) EXCELENCIA OPERATIVA

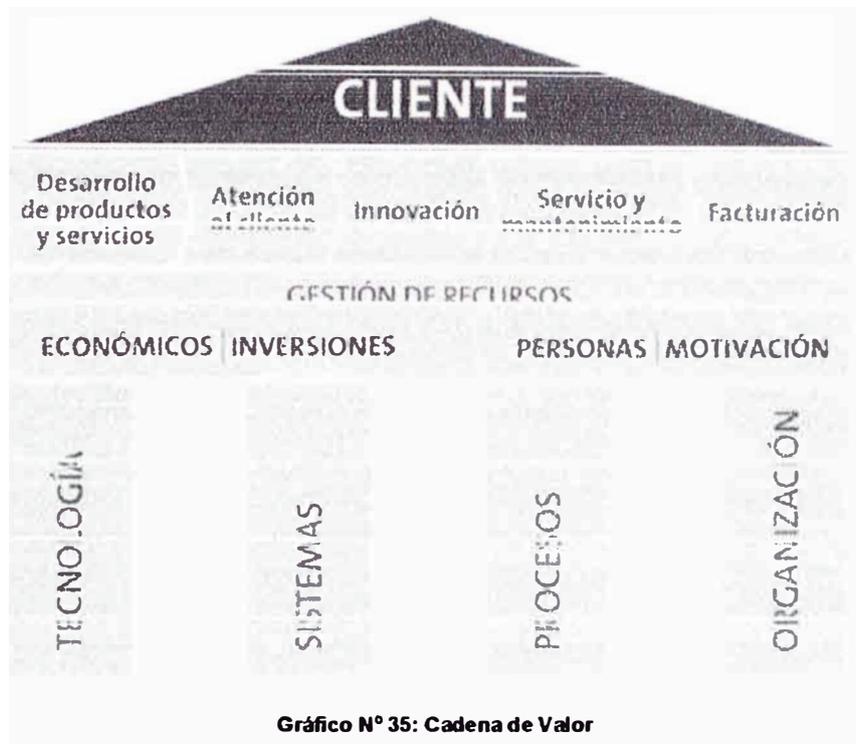
El Grupo se ha marcado como objetivo el convertirse en 2008 en "Excelente", una compañía con los mejores niveles de satisfacción del cliente, excelencia operativa (en términos de precisión en los procesos, eficiencia y rigurosa fiabilidad) gracias a un excelente grupo de profesionales con iniciativa y una enorme motivación. Para alcanzar estos objetivos, se hacen énfasis en tres líneas maestras:

- Ofrecer una calidad de servicio y una atención al cliente excepcional: desde su diseño, los servicios deben prestar atención preferente a la satisfacción del cliente. Durante todo el proceso de prestación de servicios, los parámetros de los mismos están sometidos a una revisión y mejora constantes para garantizar una óptima relación con el cliente: por ejemplo, ofreciendo algo más que la resolución de las interrupciones del servicio en tiempo record y proporcionando interfaces sin errores.
- Gestionar los equipos y la infraestructura para generar un incremento sostenible de la productividad, realizando, al mismo tiempo, una óptima elección en inversión en redes y sistemas, anticipando la convergencia tecnológica.

- Poner en marcha procesos adaptados para eliminar la complejidad de la actividad comercial, reducir los costes básicos, explotar las sinergias en las unidades, en un entorno en el que cada profesional pueda dar lo mejor de sí.

La excelencia operativa comprende un apoyo decidido de todo el Grupo e iniciativas conjuntas orientadas a la actividad comercial. Entre éstas, el “nuevo centro de trabajo del Grupo”, que se vale de la tecnología para fomentar la colaboración y la movilidad; la “racionalización de la cadena de distribución”, con ambiciosos objetivos de rotación y disminución de existencias, la “compra electrónica” y la consolidación de sistemas de planificación de recursos. Esta última iniciativa comprende proyectos de “mejora de la calidad de la banda ancha”, “gestión global de terminales”, “estándares de servicio revisados en contact centers”, “gestión de operaciones regionales”, a la vez que la integración con éxito de los activos recientemente adquiridos.

La búsqueda de la eficiencia del negocio, de la calidad del servicio y de la motivación de los empleados llevará a la empresa a un nuevo escalón de excelencia, exponente de una cultura corporativa orientada al cliente.



D) LIDERAZGO Y COMPROMISO

El Grupo está comprometido con el desarrollo profesional de sus empleados. A lo largo de 2004, el número total de horas de formación alcanzó los 9 millones. Las acciones formativas se complementan con la identificación de las competencias en el seno del grupo en su conjunto y con programas de desarrollo. En 2004, el 84% de los empleados del grupo fueron objeto de una evaluación de competencias.

El Grupo ha consolidado el uso del aprendizaje virtual como una importante herramienta para sus empleados. En 2004, la Compañía ha desarrollado nuevos

contenidos para el grupo en su conjunto relativos a las habilidades empresariales y simuladores de negocio, en los que los profesionales se enfrentan a problemas reales que fomentan el “aprendizaje mediante la acción”.

Se ha aplicado, igualmente, la innovación a las plataformas de formación, entre las que cabe destacar “Aprendizaje Móvil” y el “Sitio Empresarial de Aprendizaje Virtual”, disponibles en portugués y español. En 2004 se multiplicó por dos el número de empleados que siguieron programas formativos y el número de horas de aprendizaje virtual se incrementó en un 10%, equivalente a 11 horas anuales.

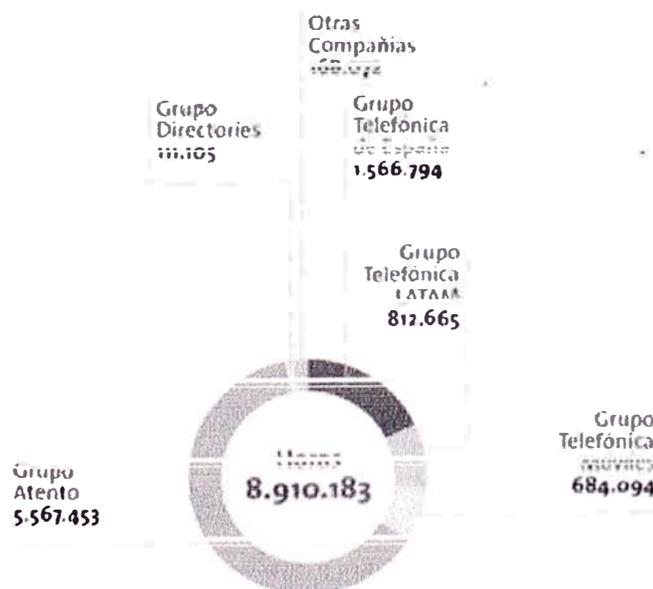


Gráfico N° 36: Horas de formación por Línea de Negocio en 2004

E) IDENTIDAD CORPORATIVA Y COMUNICACIÓN

Para el Grupo, la Identidad Corporativa y la Comunicación son piezas clave en la proyección de su visión, posicionamiento y valores a todos aquellos con los que se relaciona: clientes, empleados, accionistas, autoridades y la sociedad en su conjunto.

Nueva Estrategia y Arquitectura de Marca

El Grupo ha adoptado una nueva estrategia de marca y un nuevo modelo de arquitectura denominado "sistema de familia", cuya finalidad es la de definir funciones, criterios y estructura jerárquica entre las marcas, a través de una serie de principios de identidad y un sistema gráfico de coexistencia.

Gracias a esta nueva estrategia y este sistema de arquitectura de marca, es posible gestionar eficientemente la doble vertiente institucional y comercial del Grupo.

Funciones de la Marca

La función de las marcas comerciales consiste en complementar la marca principal aportando proximidad y frescura. Aportan, diferenciación y significación a la oferta comercial, resultando así más convincente y cercana al cliente; a la vez rejuvenecen y revitalizan la marca principal. De esta forma, el sistema favorece la comunicación de valores entre las marcas.

A. Principios de identidad:

Se trata de los atributos, valores, posicionamiento, estilo, mensajes de la marca que vertebran la identidad de la empresa principal y que se comparten en el seno del Grupo.

B. Sistema Gráfico de Coexistencia:

Se aprecia en la coexistencia de la marca principal del Grupo y las marcas comerciales con la banda azul, que sirve de conexión entre ambas marcas.

Define, además, colores, códigos, formatos, estilos y tipografías que transmiten una visión equilibrada y coherente del Grupo.

Ejemplos: Movistar:

Anexo 2: Listado de Gráficos

Gráfico N° 1: Las 3 etapas en la reforma de Telecomunicaciones

Gráfico N° 2: Participación del Sector de Telecomunicaciones en el PBI

Gráfico N° 3: Número de Usuarios de Servicios de Telecomunicaciones

Gráfico N° 4: Cadena de Valor del Sector de Telecomunicaciones

Gráfico N° 5: Ranking de empresas de telecomunicaciones en el mercado de habia hispano portuguesa

Gráfico N° 6: Organización por Líneas de Negocio del Grupo

Gráfico N° 7: Valores Corporativos del Grupo

Gráfico N° 8: Información Financiera

Gráfico N° 9: Organigrama de T Gestiona

Gráfico N° 10: Organigrama de la Gerencia de Seguridad y Protección

Gráfico N° 11: Roles existentes en el Modelo MEGON

Gráfico N° 12: Etapas de la Metodología MEGON

Gráfico N° 13: EDT del Proyecto

Gráfico N° 14: Módulos del Sistema

Gráfico N° 15: Diagrama de Casos de Uso del SIPIE – Incidencias

Gráfico N° 16: Diagrama de Casos de Uso del SIPIE – Mantenimiento

Gráfico N° 17: Diagrama de Clases del Sistema

Gráfico N° 18: Diagrama de Actividades del Caso de Uso Registro de Incidencias

Gráfico N° 19: Diagrama de Actividades del Caso de Uso Autenticación de Trabajadores

Gráfico N° 20: Diagrama de Actividades del Caso de Uso Reportes

Gráfico N° 21: Diagrama de Actividades del Caso de Uso Consultas

Gráfico N° 22: Pantalla Principal del Módulo de Administración

Gráfico N° 23: Pantalla Principal del Sistema

Gráfico N° 24: Diagrama UML del Ingreso del Usuario

Gráfico N° 25: Diagrama UML de la Administración del Sistema

Gráfico N° 26: Diagrama UML del Registro de Incidencias

Gráfico N° 27: Diagrama UML de Consultas

Gráfico N° 28: Diagrama UML de los Reportes y Estadísticas

Gráfico N° 29: Diagrama de Bases de Datos SIPIE

Gráfico N° 30: Diagrama Lógico de Datos SIPIE

Gráfico N° 31: Arquitectura del Sistema

Gráfico N° 32: Pilares para la Visión del Grupo

Gráfico N° 33: Acelerar para ser más líderes: Orientación al cliente

Gráfico N° 34: Principios de la relación del Grupo con el cliente

Gráfico N° 35: Cadena de Valor

Gráfico N° 36: Horas de formación por Línea de Negocio en 2004

Anexo 3: Listado de Cuadros

Cuadro Nº 1: Estructura de la Gerencia de Seguridad y Protección

Cuadro Nº 2: Empresas del Grupo

Cuadro Nº 3: Características Técnicas de las Alternativas

Cuadro Nº 4: Factores Técnicos para Selección de Alternativa

Cuadro Nº 5: Cuadro de Costos Alternativa 1

Cuadro Nº 6: Cuadro de Costos Alternativa 2

Cuadro Nº 7: Cuadro de Costos Alternativa 3

Cuadro Nº 8: Selección de la Alternativa

Cuadro Nº 9: Selección de la Alternativa

Cuadro Nº 10: Definición de Entregables del Proyecto

Cuadro Nº 11: Costos del Proyecto

Cuadro Nº 12: Perfiles de Usuario del Sistema