UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA

FACULTAD DE INGENIERÍA

IMPLANTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA COMISIÓN NACIONAL DE SEGUROS Y FIANZAS

T E S I S

QUE PARA OBTENER EL GRADO DE:

MAESTRO EN INGENIERÍA (SISTEMAS-PLANEACIÓN)

P R E S E N T A :

ACT. LUIS RAÚL CHIO BERMÚDEZ.

TUTOR: M.I. Mariano A. García M.

CIUDAD UNIVERSITARIA ABRIL 2011

Resumen

El presente trabajo tiene como objetivo resolver una problemática que se ha presentado en la Dirección General de Informática de la Comisión Nacional de Seguros y Fianzas **"CNSF"**, la cual se manifiesta en que los servicios informáticos que ofrece se han ido degradando con el paso del tiempo, provocando que las áreas de la CNSF no cuenten con la información para desempeñar sus labores de supervisión.

Para determinar el problema real de la CNSF, se utilizaron las herramientas de análisis de las causas raíz del problema tales como los diagramas de Causa-Efecto (Ishikawa) así como Gráficas de Pareto, con lo cual se logró identificar que los usuarios no contaban con la información de manera confidencial, oportuna e integra para desempeñar sus labores de supervisión.

Este problema se resolvió, mediante la implantación de un Sistema de Gestión de la Seguridad de la Información **"SGSI"** en la CNSF, ya que este tipo de solución es generalmente aceptada para preservar las propiedades de confidencialidad, integridad y disponibilidad de la información en las empresas.

La implantación de un SGSI implica realizar cambios profundos en la organización, para lo cual se utilizó a la planeación como una actividad fundamental para que este proceso de cambio sea controlado.

También se utilizó el enfoque sistémico y el enfoque cibernético, para entender el impacto que tendrá la implantación de un Sistema de Gestión de la Seguridad de la Información en la CNSF, ya que se identificaron a los actores y beneficiados involucrados en el sistema, también se logró conceptualizar el problema al que nos enfrentamos en donde un sistema se debe de ver como un sistema total, esto es, considerar el sistema del que forma parte (suprasistema) y sus relaciones, así como los elementos del sistema (subsistemas) en función del sistema y suprasistema que los contienen.

Y por último, se adoptó el diseño idealizado para llevar a cabo el proceso de planeación para la implantación del SGSI en la Comisión Nacional de Seguros y Fianzas, estableciendo los objetivos de conducción y las actividades que permiten realizar este cambio de manera directa, a través de programas y proyectos, que contribuyan al cambio del estado actual al estado deseado.

Introducción

El presente trabajo tiene como objetivo resolver una problemática que se ha presentado en la Dirección General de Informática de la Comisión Nacional de Seguros y Fianzas **"CNSF"**, la cual consiste en que los servicios informáticos que ofrece se han ido degradando con el paso del tiempo, provocando que las áreas de la CNSF no cuenten con la información para desempeñar sus labores de supervisión.

Como se verá más adelante, esta problemática se resolverá mediante la implantación de un Sistema de Gestión de la Seguridad de la Información "SGSI" en la CNSF, lo que implica realizar cambios profundos en la organización, para lo cual se utilizará a la planeación como una actividad fundamental para que este proceso de cambio sea controlado.

Para entender el impacto que tendrá la implantación de un Sistema de Gestión de la Seguridad de la Información en la CNSF, se utilizará el enfoque sistémico y el enfoque cibernético, tal y como se explica en el capítulo 2 Marco Conceptual y Fines de la Planeación.

En el mismo capítulo 2, se analizarán la planeación de escenarios y el diseño idealizado, con el fin de elegir uno de ellos para que sirva de referencia al proceso de planeación para la implantación del SGSI en la CNSF.

El resto de los capítulos desarrollan las diferentes etapas del diseño idealizado para la implantación de este sistema.

En el capítulo 1 Formulación de la problemática, se describe cómo opera la CNSF, se identifican los problemas que obstruyen su progreso, se realiza un diagnóstico para determinar que la solución a la mayoría de los problemas es la implantación del SGSI en la CNSF.

Para el capítulo 2 Fines de la Planeación, se establece, por parte de los planeadores, lo que quisieran que fuera la CNSF, si ésta pudiera ser lo que ellos quisieran a través de determinar el ideal, los objetivos y las metas del sistema

En el capítulo 3 Medios para la planeación, se evaluarán tres alternativas que representan estándares internacionales o marcos de referencia para implantar un Sistema de Gestión de la Seguridad de la Información, lo que permitirá posteriormente establecer los programas y proyectos necesarios para la implantación del SGSI, con los requisitos que establezca el estándar internacional seleccionado.

En el capítulo 4 Planeación de recursos, se determinarán la cantidad de recursos personales, materiales y económicos necesarios para ejecutar las actividades que se han establecido en los programas y proyectos referidos para la implantación del sistema.

Y por último en el capítulo 5 Implantación y Control, se debe decidir quién será responsable de hacer qué y cuándo, adicionalmente se realizará la identificación de variables, la definición de los criterios de medición y se diseñaran los indicadores, que permitan evaluar y adoptar las acciones correspondientes cuando se presenten desviaciones a los planes y a la planeación

Capítulo 1. Formulación de la problemática

1.1. La CNSF.

La CNSF (Comisión Nacional de Seguros y Fianzas) es un organismo desconcentrado de la SHCP (Secretaría de Hacienda y Crédito Público), el cuál tiene como misión el de supervisar de manera eficiente, que la operación de los sectores asegurador y afianzador se apeguen al marco normativo, preservando la solvencia y estabilidad financiera de las instituciones, para garantizar los intereses del público usuario, así como promover el sano desarrollo de estos sectores con el propósito de extender la cobertura de sus servicios a la mayor parte posible de la población.

La CNSF se puede representar dentro del sector gobierno como se muestra en la figura 1.1.

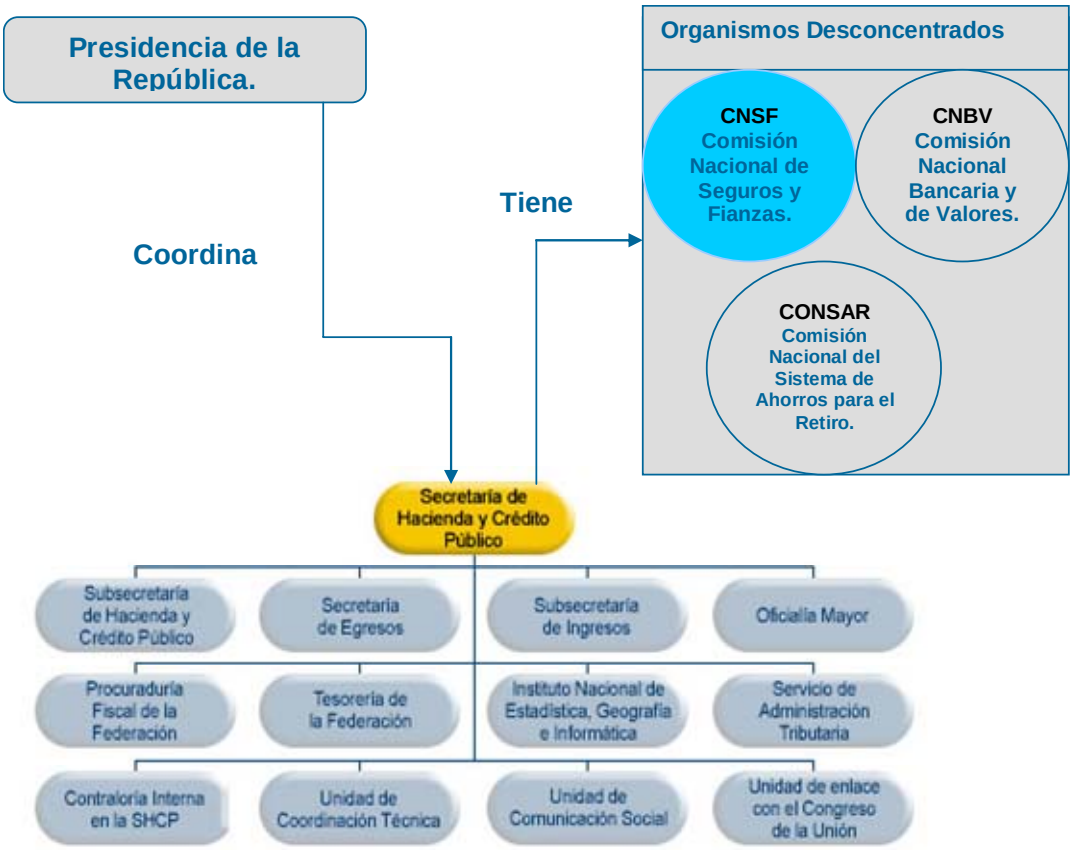


Figura 1.1. La CNSF dentro del sector gobierno.

Debido a los cambios constantes de la ley en materia de regulación de seguros y fianzas, la Comisión Nacional de Seguros y Fianzas tiene que estar haciendo los ajustes necesarios a los procesos, procedimientos y circulares, para que las áreas del organismo realicen la supervisión conforme se estipula en dicha ley.

Como se puede observar las áreas que integran la CNSF, se muestran en la figura 1.2.

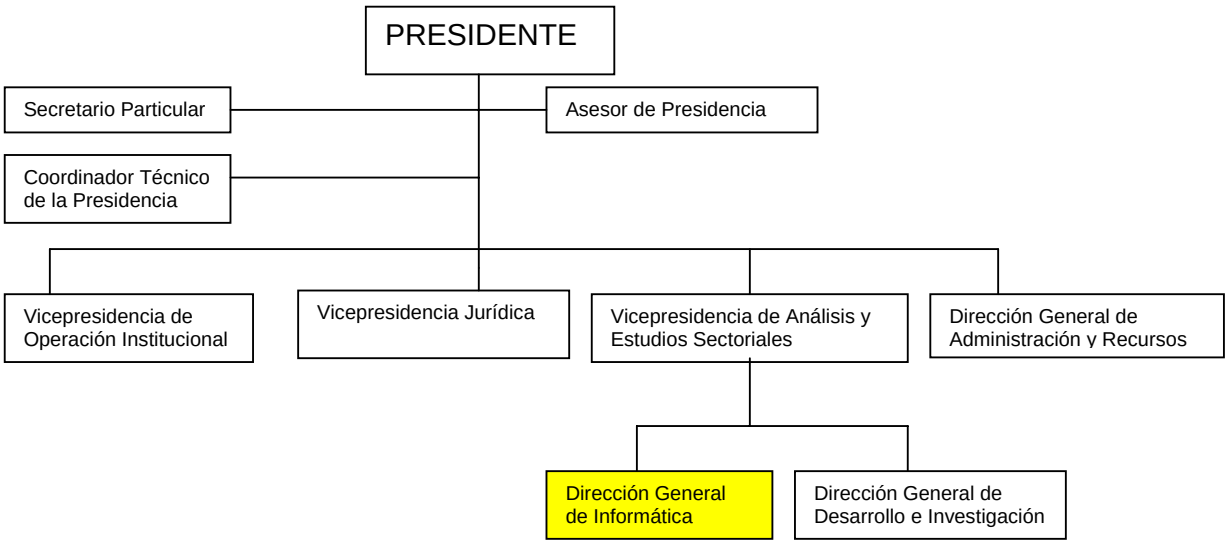


Figura 1.2. Organigrama Comisión Nacional de Seguros y Fianzas

Estos cambios a la ley, se traducen también en ajustes a la plataforma de tecnologías de información de la CNSF, ya que como pasa en la mayoría de las empresas, la operación de este organismo se sustenta en gran parte de dicha plataforma, como son computadoras, redes, sistemas de información, correo electrónico e Internet, por mencionar algunos.

Es importante señalar que la Dirección General de Informática es la encargada de dotar a la Comisión de esta plataforma de tecnologías de información que le permitan cumplir a la CNSF eficientemente con sus funciones de supervisión.

La estructura organizacional de la DGI, se muestra en la Figura 1.3

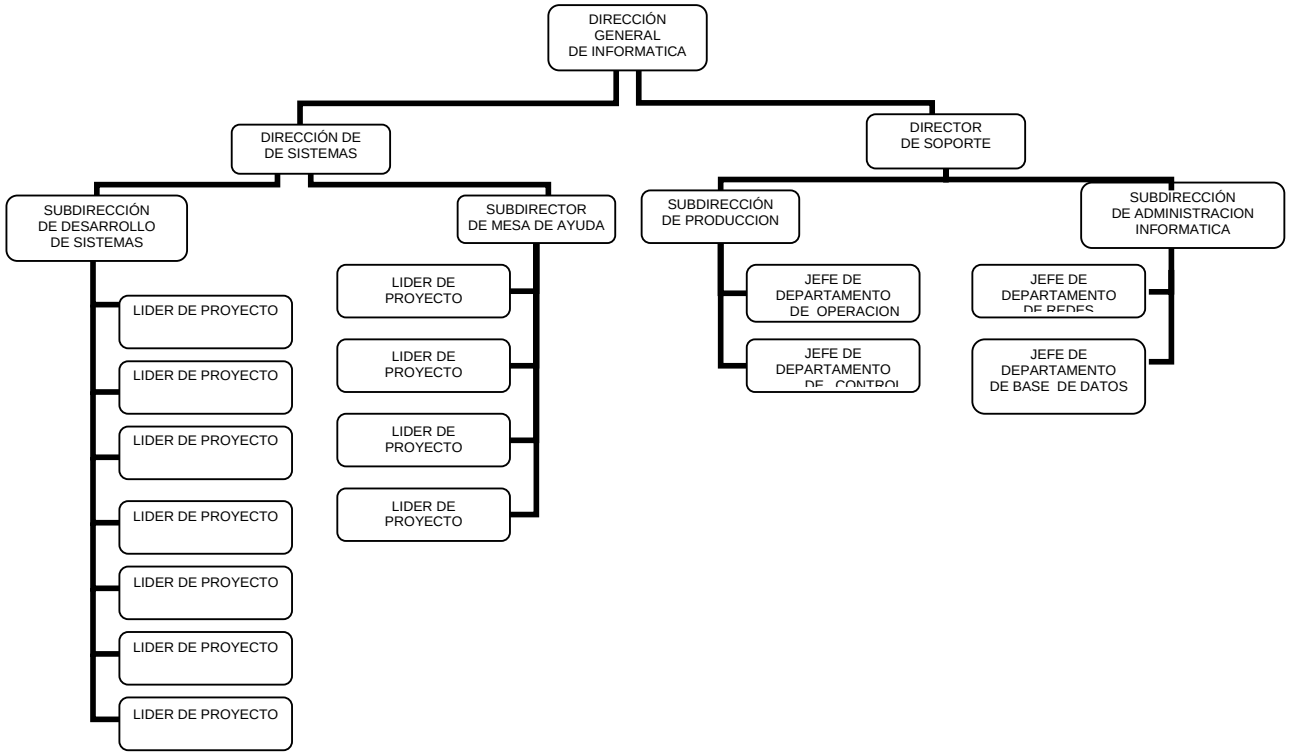


Figura 1.3. Estructura de la Dirección General de Informática.

1.2. Investigación de lo real

Evolución de la Dirección General de Informática

La operación de la DGI desde 1995 a 2010, ha ido incrementado su complejidad, debido al número de componentes y servicios que están interactuando, esta operación se puede clasificar en las siguientes áreas:

- Infraestructura
- Sistemas
- Servicios
- Desarrollo de Sistemas

Desde el punto de vista de lo cambios en la infraestructura, ésta ha crecido en el número de servidores, capacidad de almacenamiento, número de computadoras personales y diferentes formas de redes para compartir información, tal y como lo muestra la tabla 1.1.

1995	2000	2008
Infraestructura		
▪ 2 Servidores HP 9000 Unix	▪ 2 Servidores HP 9000 Unix ▪ 7 Servidores Intel	▪ 2 Servidores HP 9000 Unix ▪ 12 Servidores Intel ▪ Sistema de Almacenamiento ▪ Robot de Respaldos
▪ 10 redes 5 nodos en promedio (aisladas) Novell	▪ Red Institucional 400 nodos ▪ Red con Delegaciones Regionales	▪ Red Institucional 520 nodos ▪ Red inalámbrica ▪ VPN con Delegaciones Regionales, Villalpando y Universidad
▪ 222 PC y 10 Lap Tops	▪ 320 Pc y 35 Lap Tops	▪ 440 Pc y 75 Lap Tops ▪ 80 impresoras ▪ 7 proyectores
		▪ Site: ▪Aire Acondicionado ▪Sistema contra incendios ▪UP's Redundante

Tabla 1.1. Infraestructura en la DGI

Con respecto a la evolución de los sistemas, éstos cada vez apoyan más actividades sustantivas en la CNSF, tal y como se muestra en la tabla 1.2.

1995	2000	2008
Sistemas		
▪ BD Oracle y SISINF	▪ BD Oracle y Express	▪ BD Oracle y Express ▪ Cognos (BI)
▪ 55 Sistemas de captura en clipper		
▪ SIIF Seguros y SIIF Fianzas	▪ SIE y SIIF Unificado	▪ SIE y SIIF Unificado
▪ Inversiones, Inmuebles, CMG, … ▪ 13 Sistemas de Gestión a través de disquete ▪ 9 Sesa's	▪ SIRH y SIRF ▪ Sistema de digitalización de cédulas de agentes	▪ SIRH y SIRF ▪ Digitalización cédulas agentes ▪ Acreditación de agentes ▪ Sistema de Despacho ▪ Control de Gestión ▪ Registro de Productos ▪ SEIVE, SITI ▪ SVC ▪ Remate de Valores ▪ IPR ▪ Control de Sanciones ▪ Módulos de Explotación

Tabla 1.2. Sistemas en la DGI

En relación a los servicios que ofrece la Dirección General de Informática, éstos se han incrementado de manera importante, complicando la operación de la dirección, estos servicios por periodo se mencionan en la tabla 1.3.

1995	2000	2008
Servicios		
▪ Soporte a los usuarios	▪ Soporte a los usuarios	▪ Soporte a los usuarios
▪ Mantenimiento a los sistemas y nuevos desarrollos	▪ Mantenimiento a los sistemas y nuevos desarrollos	▪ Mantenimiento a los sistemas y nuevos desarrollos
▪ Operación de los sistemas	▪ Operación de los sistemas	▪ Operación de los sistemas
	▪ Comunicaciones ▪ Internet ▪ Mail Institucional	▪ Comunicaciones ▪ Internet ▪ Mail Institucional ▪ Antivirus
	▪ Página Web	▪ Página Web
		▪ Red con Delegaciones
		▪ Ventanilla Única
		▪ Exámenes de Acreditación ▪ Escaneo y grabado de CD's
		▪ Seguridad de la información ▪ Continuidad de los servicios

Tabla 1.3. Servicios en la DGI

Y por último, la actividad para desarrollar sistemas de información requiere de mayores conocimientos y especialización, ya que de sistemas utilizados por un sólo usuario (sistemas locales) ahora se requieren de sistemas utilizados por varios usuarios en diferentes partes del mundo (sistemas en Internet). Adicionalmente, se requieren utilizar metodologías para establecer formas de trabajo en común para varias personas, que realizan actividades en el desarrollo de sistemas cada vez más complejas.

Un mayor detalle de cómo ha evolucionado esta disciplina en la CNSF, se presenta en la tabla 1.4.

1995	2000	2008
Desarrollo de Sistemas		
▪ Clipper, SISINF y Oracle	▪ Delphi, Clipper y Oracle	▪ Oracle, Java, Lotus Script
▪ Sistemas locales con propósitos específicos	▪ Sistemas en red, para varias áreas	▪ Sistemas en Internet (usuarios externos), y de propósito gral.
▪ Dependían de la creatividad del programador ▪ No pruebas	▪ Se controla el desarrollo de los programadores, pero de manera intuitiva ▪ Primeros sistemas que para su desarrollo requerían más de un programador (Mayor complejidad)	▪ Implementación de la Metodología RUP (Mejorar ciclo de desarrollo de sistemas) ▪ Iterativo e incremental ▪ Adm. de Requerimientos ▪ Modelado visual ▪ Adm. de la Configuración ▪ Aseguramiento de la Calidad ▪ Arquitectura por componentes
		▪ Sist. Inteligencia de Negocio
		▪ Integración de sistemas
		▪ Administración de Man -Power ▪ Administración de Proyectos ▪ Inspección de código

Tabla 1.4. Desarrollo de Sistemas en la DGI

Como se puede observar en los últimos años, la Comisión Nacional de Seguros y Fianzas ha alcanzado un notable crecimiento en el tamaño de la infraestructura tecnológica, un aumento en el número de los servicios informáticos y una mayor complejidad en la manera de desarrollar sistemas.

1.3. Planteamiento de la Problemática.

Como sabemos la operación cotidiana de las empresas se desarrolla principalmente con base en la información, esta información hoy en día generalmente se almacena, transporta y procesa en medios informáticos, por lo que las operaciones cotidianas de las empresas dependen en gran medida de las computadoras y de los sistemas de información.

Dado lo anterior, la Dirección General de Informática se encuentra ante la siguiente problemática ya que los servicios informáticos que ofrece, se han ido degradando con el paso del tiempo, provocando que las áreas de la CNSF no cuenten con la información de manera confidencial, oportuna e integra para desempeñar sus labores de supervisión.

De tal manera que los síntomas más frecuentes que se presentan cuando se da un servicio informático, por mencionar algunos, son:

- Caída frecuente de servicios (Mail, Portal, Internet)
- Lentitud en la red (copiar información, ejecutar aplicaciones)
- No se atiende oportunamente o no se corrige realmente el problema
- Capacidad de respuesta insuficiente para mantener y desarrollar aplicaciones
- Las aplicaciones cumplen parcialmente con las necesidades del usuario

- Faltan competencias
- Falta el aseguramiento de los procesos de negocio
- Falta incrementar la confiabilidad en la operación

Los cuáles traen como consecuencia que se tenga que hacer trabajo duplicado o estar atendiendo tareas urgentes, lo cuál implica tiempo, recursos para su corrección y sobre todo una mala imagen de la DGI que pone en duda la calidad de sus servicios.

Lo anterior, tampoco permite que los proyectos prioritarios de la DGI se les de una atención adecuada, ya que se distrae al personal de la dirección para atender estas tareas urgentes.

Se han realizado algunos intentos de diagnóstico para precisar las causas de las fallas y se han tomado acciones correctivas de manera casuística, sin embargo, no se ha establecido algún procedimiento general de prevención, método o guía que permita analizarlos de manera sistemática y así reducir el número de errores en los servicios.

Actualmente, la mayoría de los servicios se establecen sin definir políticas, procesos, procedimientos, controles y niveles de servicio, por lo que el servicio se realiza conforme al criterio de la persona que atiende, lo cual provoca que se cometan errores u omisiones que impacta en la calidad de los mismos.

1.4. Evaluación y diagnóstico

1.4.1. La situación actual de los servicios informáticos en la Comisión Nacional de Seguros y Fianzas considerando la seguridad de la información

En la Dirección General de Informática no existe un área específica de seguridad de la información, que se encargue de preservar los atributos de confidencialidad, integridad y disponibilidad de la información. Cada área de esta dirección se ocupa de proveer los servicios informáticos a los usuarios, pero sin considerar de manera integral y estructurada la seguridad de la información que se debe considerar en estos servicios.

Más aún los procesos, procedimientos y políticas utilizados para proporcionar estos servicios, tampoco consideran requisitos de seguridad de la información.

De tal manera, que al proporcionar un servicio, como por ejemplo el servicio de red para los empleados de la Comisión Nacional de Seguros y Fianzas, sin considerar desde un inicio requisitos de seguridad como el control de acceso, se le pueden dar privilegios a ese usuario para consultar información sensible, de tal manera que esa persona podría alterar o divulgar la información, perjudicando la operación y muy probablemente la imagen de la CNSF.

Esto genera que se realicen actividades no planeadas y nuevos esfuerzos de trabajo para corregir estos problemas asociados a la seguridad de la información, que provocan malos resultados por las interrupciones a los servicios que se proporcionan a las áreas usuarias de la CNSF.

1.4.2. Identificación de las operaciones que fallan

Como identificación de las operaciones que fallan se realizaron las siguientes actividades:

- Se realizó un cuestionario diseñado por la Dirección General de Informática que se aplicó a las áreas internas de la CNSF para detectar los problemas más frecuentes y que impactan en su trabajo cotidiano.

- Se consultó las solicitudes de servicio reportadas por los usuarios de los últimos 12 meses (en la sección de Anexos, se presenta una muestra)[1]

- Se hizo una reunión con el personal de la DGI en donde cada uno indicó cuáles son esas operaciones que están fallando. Se manifestaron afirmaciones acerca de los servicios informáticos que se ofrecen, lo cual generó una tormenta de ideas.

Para analizar toda esta información y tratar de establecer las causas, las interrelaciones entre los factores y lograr una explicación más profunda y amplia del problema, primero se clasificó y agrupó esta información y posteriormente se realizó el diagrama causa-efecto, que se muestra en la figura 1.4.

[1] Comisión Nacional de Seguros y Fianzas. Solicitudes DGI-H. (2008)

Causas del problema

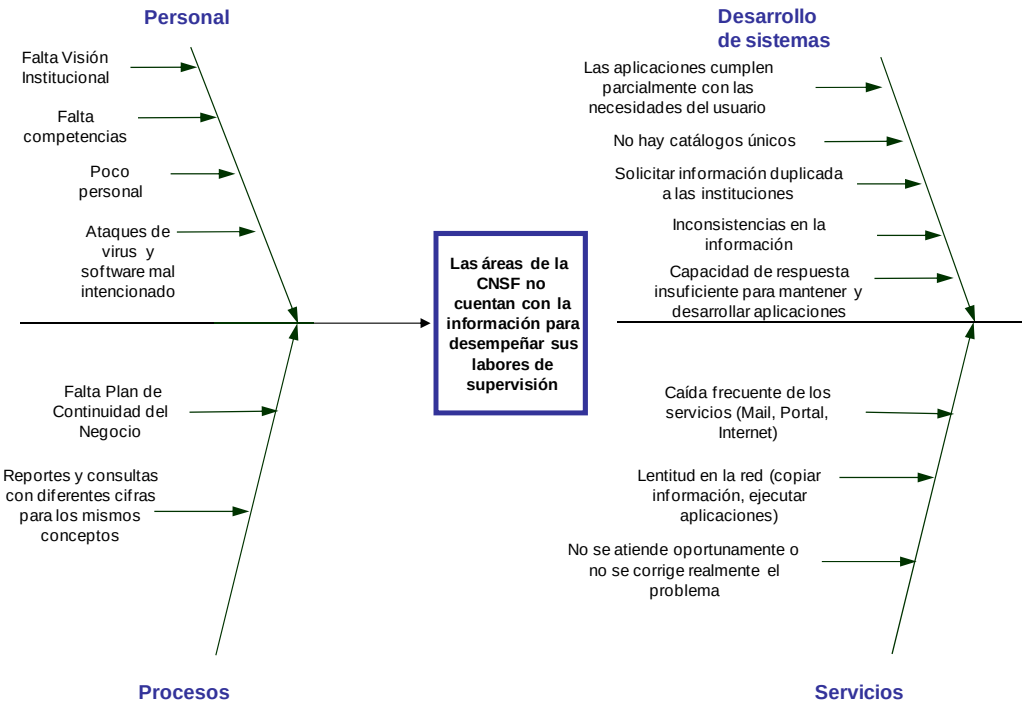


Figura 1.4. Diagrama Causa-Efecto

Derivado del análisis, se concentraron 14 fallas o factores que intervienen en los servicios de TI, los cuales provocan que éstos no se realicen correctamente.

1. No se atiende oportunamente o no se corrige realmente el problema
2. Capacidad de respuesta insuficiente para mantener y desarrollar aplicaciones
3. Las aplicaciones cumplen parcialmente con las necesidades del usuario
4. Ataques de virus y software mal intencionado
5. Lentitud en la red (copiar información, ejecutar aplicaciones)
6. Caída frecuente de servicios (Mail, Portal, Internet)
7. Falta competencia
8. No hay catálogos únicos
9. Falta Plan de Continuidad del Negocio
10. Reportes y consultas con diferentes cifras para los mismos conceptos
11. Inconsistencias en la información
12. Poco personal
13. Solicitar información duplicada a las instituciones
14. Falta Visión Institucional

1.4.3. Análisis de causas de las fallas.

Derivado de las fuentes de información citadas en la sección anterior, se obtuvo la frecuencia de las operaciones que fallaron en los últimos 12 meses de todos los servicios informáticos que ofrece la Dirección General de Informática, las cuales se muestran en la tabla 1.5.

# DE FALLA	FALLAS QUE SE PRESENTAN EN LOS SERVICIOS QUE OFRECE LA DGI	FRECUENCIA
6	Caída frecuente de servicios (Mail, Portal, Internet	225
11	Inconsistencias en la información	165
4	Ataques de virus y software mal intencionado	152
5	Lentitud en la red (copiar información, ejecutar aplicaciones)	143
13	Solicitar información duplicada a las instituciones	26
3	Las aplicaciones cumplen parcialmente con las necesidades del usuario	24
9	Falta Plan de Continuidad del Negocio	20
8	Catálogos únicos	18
10	Reportes y consultas con diferentes cifras para los mismos conceptos	16
1	No se atiende oportunamente o no se corrige realmente el problema	15
2	Capacidad de respuesta insuficiente para mantener y desarrollar aplicaciones	12
14	Falta Visión Institucional	12
12	Poco Personal	12
7	Falta competencias	11

Tabla 1.5. Fallas que se presentan en los servicios que ofrece la DGI

Se realizo un "Análisis de Pareto" para identificar cuál es el 80% que se mejorará trabajando sobre el 20% de las fallas, este análisis se presenta en la figura 1.6.

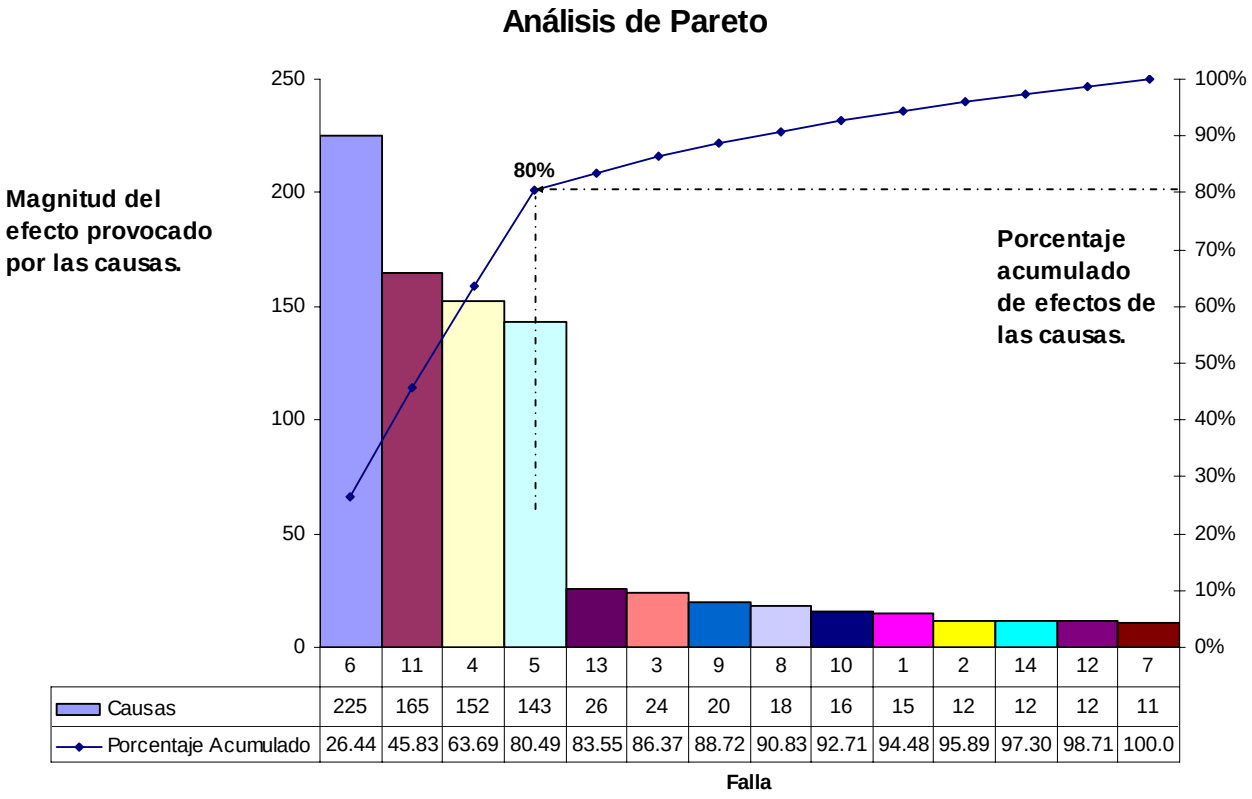


Figura 1.6. Análisis Pareto

De acuerdo al diagrama anterior, las fallas que representan el 80% que se mejorará, son las siguientes:

6. Caída frecuente de servicios (Mail, Portal, Internet)

11. Inconsistencias en la información

4. Ataques de virus y software mal intencionado

5. Lentitud en la red (copiar información, ejecutar aplicaciones)

Estas fallas repercuten directamente **con la información que se utiliza en las áreas de la Comisión Nacional de Seguros y Fianzas** para desempeñar las funciones de supervisión que tiene encomendadas por la ley.

En cuanto a la fallas: 5. Lentitud en la red y 6. Caída frecuente de servicios, se relaciona con el atributo de la disponibilidad de la información, que tiene como objetivo asegurar que los usuarios autorizados tengan acceso a la información

y a los activos asociados cuando se requiera.

En relación a la falla 11. Inconsistencias en la información, se asocia con el atributo de integridad de la información, que pretende salvaguardar la exactitud y completez de la información y los métodos de su procesamiento.

Y por último, respecto a la falla 4. Ataques de virus y software mal intencionado, éste corresponde con el atributo de la confidencialidad que asegura que la información sea accesible sólo para quienes estén autorizados para ello.

Para responder antes estas fallas que están relacionadas con proteger la información en cuanto a los atributos de confidencialidad, integridad y disponibilidad, es necesario implantar un **Sistema de Gestión de la Seguridad de la Información** en la Comisión Nacional de Seguros y Fianzas, que tenga como fines asegurar la continuidad del negocio, minimizar el impacto al negocio, maximizar el retorno de la inversión y mejorar las oportunidades del negocio.

Estas fallas provocan una alta insatisfacción entre los usuarios de la CNSF, las cuales son notificadas tanto por los usuarios internos, como por los usuarios externos, que prácticamente son el sector asegurador.

A través de la Asociación Mexicana de Instituciones de Seguros (AMIS) se realizan comités bimestrales, en donde su principal función es que la CNSF presente las modificaciones a los sistemas informáticos derivados de los cambios en la regulación de seguros, de tal manera que las compañías de seguros puedan cambiar sus sistemas de una manera oportuna.

Sin embargo, en dicho comité también la AMIS presenta inconformidades que tienen las compañías de seguros acerca de los servicios informáticos que ofrece la Dirección General de Informática, como por ejemplo, el servicio para la entrega de la información que sirve para que las compañías envíen información a la CNSF a través de Internet, el cual frecuentemente tiene fallas de disponibilidad, que repercute en que las compañías no puedan entregar su información y las áreas internas no puedan hacer las funciones de supervisión eficientemente.

1.5. Escenarios de Referencia

Por lo tanto, en caso de que no haya una intervención en el sistema involucrado y su medio ambiente, esto es, sin que haya ningún cambio en las tendencias, los posibles escenarios de referencia que pueden darse como consecuencia de la problemática expuesta son:

- Pérdida de confianza (imagen) de la CNSF hacia los clientes y del sector asegurador y afianzador

- Pérdida de productividad de las áreas internas de la CNSF, que se encargan de supervisar directamente a las instituciones de seguros y fianzas.

- Altos costos laborales por contención, reparación y reconstrucción de la información, en caso de pérdida de la misma.

- Aumento en primas de seguro por no contar con los mecanismos de seguridad físicos en la Comisión Nacional de Seguros y Fianzas.

- Aumento en gastos legales por demandas de terceros

- Multas o castigos por infringir alguna Ley para los empleados de la CNSF.

1.6. Justificación y Objetivo de la tesis

Las empresas se han vuelto más competitivas y se debaten entre ellas por entregarnos productos y servicios más vanguardistas con tan sólo darle clic a un botón de nuestra PC, del control remoto de la televisión, de nuestro celular o de los ahora electrodomésticos inteligentes.

Toda esta tecnología ha aumentado la cantidad de información que procesamos, intercambiamos y almacenamos, y por lo tanto han aumentado los riesgos asociados con el uso de la misma. Ahora se vive en un mundo donde hay secuestros virtuales, donde se reciben correos electrónicos intentando obtener nuestra clave de acceso al banco en línea, donde los ladrones entran a través de un cable de red o por la red inalámbrica.

Se han tenido que aprender cosas a una velocidad marcada por el ritmo de los avances de la tecnología, sin tener suficiente tiempo para poder asimilar o incluso visualizar las consecuencias de su uso.

Es por todo lo anterior, que la velocidad de asimilación y entendimiento de la seguridad de la información en las empresas va en crecimiento constante. Hay que observar todos los eventos o conferencias tanto nacionales e internacionales que se proporcionan alrededor del tema de seguridad de información: Bsecure, Infosecurity Forum, Día de la Seguridad de la Información convocada por la Secretaría y Hacienda y Crédito Público, Conferencia anual Latinoamericana de Seguridad de Información, etc.

La seguridad de la información consiste en la preservación de las propiedades de confidencialidad, integridad y disponibilidad de nuestra información. Se deben considerar las necesidades reales que cada organización o individuo requieren; de acuerdo al valor que le den a su información; hay que analizar los riesgos a los que ésta se expone para poder implantar soluciones, ya sean estratégicas, operativas o técnicas; hay que planear qué vamos a hacer cuando algo falle; hay que monitorear que las soluciones estén cumpliendo con los propósitos para los cuales fueron implantadas; y finalmente, este ciclo hay que repetirlo periódicamente para mantenernos vigentes y acordes a la realidad en que vivimos.

Desde hace años se han hecho grandes esfuerzos en el desarrollo de estrategias para la administración de la seguridad de la información y gracias a ello es que actualmente contamos con estándares internacionales, como el

ISO27001, que nos ayuda a encontrar ese enfoque estructurado y administrado para proteger la información con base en la implantación de un sistema de gestión de la seguridad de la información (SGSI)

De alguna u otra manera todos hacemos una administración de la seguridad de nuestra información, sin embargo, la formalidad y los recursos que invertimos en ella dependen en gran medida de la importancia que tiene la información para cada uno, ya sea en términos de individuos o de organizaciones, del nivel de riesgo con el que queremos convivir y, en el peor de los casos, de una eventualidad que nos haya hecho abrir los ojos a las consecuencias de no hacer un esfuerzo mayor para proteger nuestra información.

Actualmente, casi todas las organizaciones cuentan con alguna herramienta de seguridad como un antivirus y un firewall, y sin embargo, siguen teniendo problemas para proteger su información, ya que éstas son sólo un medio pero no el fin. Mas allá de contar con lo último en tecnología para proteger nuestra información, se requiere entender el por qué y para qué de dicha tecnología, y es en ese momento cuando empezamos a administrar formalmente la seguridad de la información mediante un sistema.

Una organización mejora su nivel de seguridad cuando empieza a implantar soluciones más administrativas, como el uso de políticas y procedimientos, que complementan las soluciones técnicas con las que ya contaba. Madurar un sistema de gestión de la seguridad de la información, en última instancia es un cambio cultural y, como todo camino hacia la madurez, requiere de tiempo, esfuerzo y paciencia, pero una vez que lo adoptamos y nos hacemos de una disciplina, los resultados se podrán percibir desde el momento en que empezamos a aplicar lo que sabemos y a hacer lo que queremos.

Ante estas circunstancias, el presente trabajo tiene como objetivo resolver la problemática que se presenta en la Dirección General de Informática de la Comisión Nacional de Seguros y Fianzas **“CNSF”**, la cual se manifiesta en que los servicios informáticos que ofrece se han ido degradando con el paso del tiempo, provocando que las áreas de la CNSF no cuenten con la información para desempeñar sus labores de supervisión.

Como se analizó anteriormente, el problema real de la CNSF consiste en que los usuarios no cuentan con la información de manera confidencial, oportuna e integra para desempeñar sus labores de supervisión.

Este problema se resolverá, mediante la implantación de un Sistema de Gestión de la Seguridad de la Información **“SGSI”** en la CNSF, ya que este tipo de solución es generalmente aceptada para preservar las propiedades de confidencialidad, integridad y disponibilidad de la información en las empresas.

En dicho sistema, se establecen los programas y proyectos de un SGSI, tales como Análisis de Vulnerabilidades y Evaluación de Controles, Análisis de Riesgos, Adquisición e instalación de herramientas, Desarrollo de Normatividad, Establecimiento de la Función de Seguridad y si se requiere que el sistema se certifique bajo el estándar ISO 27001, se pone a disposición una fase de Certificación y Acreditación.

Por lo tanto, la implantación de un SGSI en la CNSF, mejorará los servicios informáticos y a su vez incrementará los niveles de seguridad y protección de la información que ofrece la Dirección General de Informática, aumentando la productividad de los empleados de la CNSF y recuperando la confianza del sector asegurador.

Capítulo 2. Marco Conceptual y Fines de la Planeación

2.1. Marco Conceptual

Como primer paso, se necesita entender la naturaleza integral de un Sistema de Gestión de la Seguridad de la Información en la Comisión Nacional de Seguros y Fianzas, por lo que se utilizará el enfoque sistémico y el enfoque cibernético.

El enfoque sistémico ayudará a comprender los problemas que se presenten como un todo desde el punto de vista de sistema. Existen estudios realizados por Checkland y Ackoff en donde se considera el estudio de los sistemas como un todo.

Checkland[2] en general plantea la solución de problemas dentro de las organizaciones, pero sin embargo muestra a detalle una metodología para estructurar los problemas, en los cuáles se debe identificar:

- Considerar las actividades mínimas para resolver el problema y de ahí partir en subsistemas.
- Visión y razón del sistema.
- Los actores que están involucrados en el sistema y beneficiados
- Las conexiones que existen entre los sistemas, la dirección, cuales son necesarios o no.
- Desglosar la parte de operación del sistema (identificar cuáles son las entradas y cuál es el resultado que se espera y produce un beneficio.)

También la parte que maneja mucho es la percepción y lo más importante de todo es la conceptualización bien clara del problema que se requiere representar, ya que si no se tiene claro podría causar errores en nuestras definiciones así como las relaciones que existen entre ellas.

Por otra parte el enfoque cibernético[3], dará una pauta para definir los subsistemas que integran a un sistema, permitiendo visualizar los mecanismos de control, con la consecuente definición de procesos de gestión. En particular, se distinguen dos subsistemas que integran a un sistema, uno de ellos es el conducido y el otro, el conducente[4].

El llamado *controlado o conducido*[5], es un subsistema que se encarga de realizar las actividades productivas, las cuales son necesarias para lograr los objetivos generales del sistema.

Por otro lado, el subsistema de control, también conocido por los nombres de *subsistema de gestión* o *conducente*, como el encargado de realizar las actividades de organización, regulación y control para lograr cambios de estado

[2] Checkland, P. Pensamiento de Sistemas, Práctica de Sistemas. 1993.

[3] **Beer S.** *What is Cybernetics?* Kibernetes, Emerald Editors, Vol. 31, Issue 2, 2002, pp. 209-219

[4] Gelman O. & Negroe G. La planeación como un proceso básico en la conducción. Revista de la Academia Nacional de Ingeniería, 1982, Vol. I No. 4, México, pp. 253- 270

[5] Gelman O. Desastres y Protección Civil: Fundamentos de Investigación Interdisciplinaria. Universidad Nacional Autónoma de México, Dirección General de Asuntos de Personal Académico, Instituto de Ingeniería, 1996, pp. 158.

en el subsistema conducido (lo cual podría ser también, ningún cambio), a través de un proceso de gestión.

Para que en el subsistema de gestión se tomen decisiones adecuadas, se requiere de conocer el estado actual del subsistema conducido, obteniendo conocimiento mediante un flujo de información, a través de relaciones de información del conducido al conducente.

Además, el subsistema de gestión obtiene información de otros subsistemas, ya sea en el *plano*[6] conducente y/ o conducido. Cuando en el subsistema de gestión se toman decisiones, se transmiten mediante relaciones de ejecución, del conducente al conducido, con el propósito de que el conducido realice las decisiones tomadas.

De tal manera que utilizando estos dos enfoques, la implantación de un Sistema de Gestión de la Seguridad de la Información en la CNSF se puede representar identificado a la Dirección General de Informática como el objeto de estudio y el objeto conducido, al SGSI como un objeto conducente y a la CNSF como el suprasistema de la DGI.

Lo anterior, se puede representar mediante la figura 2.1.

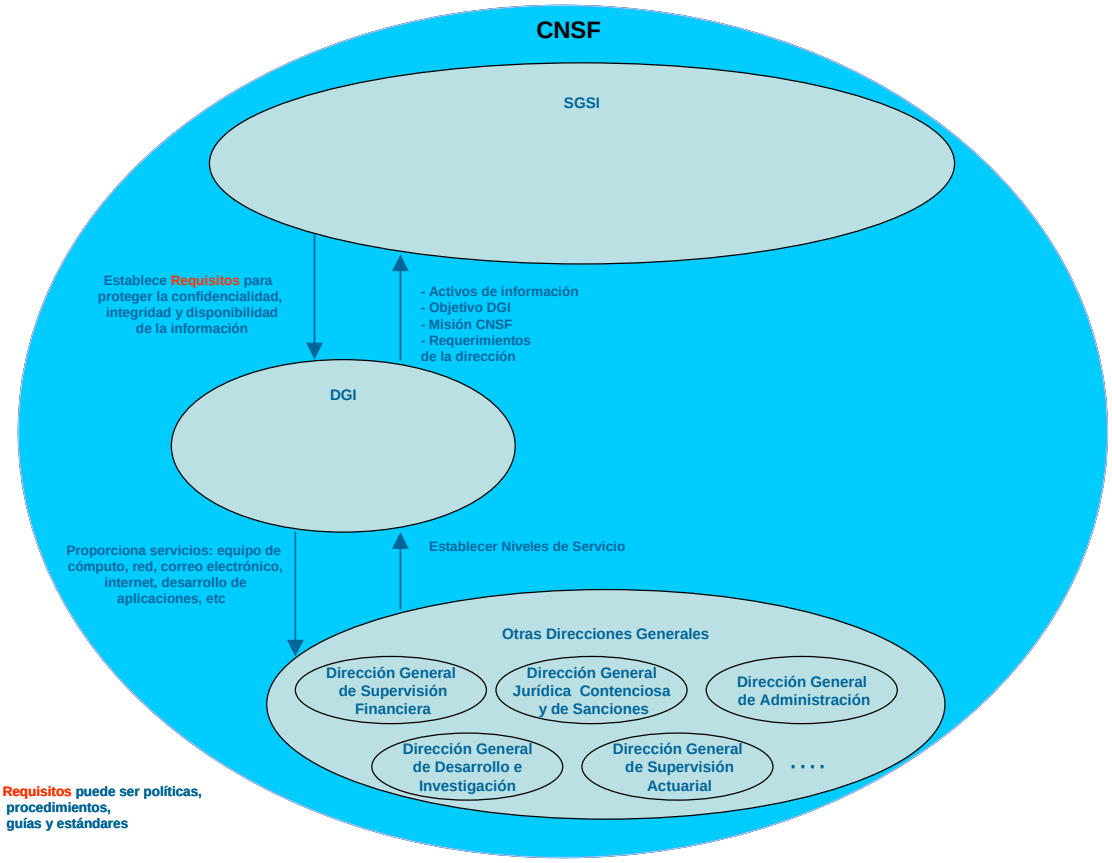


Figura 2.1. Implantación de un SGSI en la CNSF

[6] Flood R. L., Jackson M.C. Creative Problem solving: Total Systems Intervention. John – Wiley & Sons, 2002, pp. 250.

Adicionalmente, para poder entender la retroalimentación entre el SGSI y la Dirección General de Informática, debemos partir de la misión del suprasistema que es la Comisión Nacional de Seguros y Fianzas, la cual ya fue mencionada anteriormente:

"La CNSF es un organismo desconcentrado de la SHCP (Secretaría de Hacienda y Crédito Público) el cuál tiene como misión el de supervisar de manera eficiente, que la operación de los sectores asegurador y afianzador se apeguen al marco normativo, preservando la solvencia y estabilidad financiera de las instituciones, para garantizar los intereses del público usuario, así como promover el sano desarrollo de estos sectores con el propósito de extender la cobertura de sus servicios a la mayor parte posible de la población."

Con esta referencia, se podrá comprender el objetivo y las funciones que se le han encomendado a la DGI, para que contribuyan con el cumplimiento de su misión.

Objetivo de la Dirección General de Informática:

La Dirección General de Informática es la encargada de dotar a la CNSF, de la plataforma de tecnologías de información, que le permitan a la comisión, cumplir eficientemente con sus funciones de supervisión.

Para cumplir con el objetivo mencionado, se requiere realizar las siguientes funciones:

A. Planear y organizar la operación informática de la CNSF, así como establecer programas y esquemas generales de manejo de información y de equipamiento.

B. Coordinar la definición y desarrollo de los programas anuales de procesamiento de información y desarrollo de sistemas.

C. Determinar los programas anuales de adquisiciones de bienes informáticos y elaborar el presupuesto correspondiente que atienda las necesidades de expansión y sustitución de equipos.

D. Apoyar en la definición de la estrategia en materia de cultura informática institucional.

E. Representar a la comisión ante los diversos foros que en materia de informática requieran de su participación.

F. Analizar procedimientos y propiciar la automatización de la entrega de la información periódica que las instituciones de seguros y fianzas, deben presentar a la comisión.

G. Constituirse como ventanilla única de recepción de la información que de forma periódica entregan las instituciones de seguros y fianzas a la comisión para efectos de supervisión en medios magnéticos y electrónicos.

H. Proporcionar los sistemas informáticos de la comisión a los usuarios internos y externos, y dar el soporte y la accesoria que requieran.

I. Instalar y mantener en operación los bienes y servicios informáticos de la comisión.

J. Tramitar, proponer y, en su caso, imponer de conformidad con el acuerdo delegatorio correspondiente, las sanciones previstas en la ley general de instituciones y sociedades mutualistas de seguros y la ley federal de instituciones de fianzas, por violaciones a dichos ordenamientos y a las disposiciones administrativas que de ellas emanen, relacionadas con las atribuciones de su competencia.

K. Recibir y resolver en el ámbito de su competencia, sobre los programas de autocorrección que presenten las instituciones y sociedades mutualistas de seguros y las instituciones de fianzas.

L. Realizar la inscripción de tramites, en el registro federal de tramites y servicios de la comisión federal de mejora regulatoria, en el área de su competencia.

M. Proponer reformas a las leyes de la materia y demás ordenamientos legales aplicables, preparando el proyecto de manifestación de impacto regulatorio (MIR) correspondiente.

N. Establecer políticas, normas y procedimientos internos, en materia de seguridad informática, así como los recursos tecnológicos relacionados con los mecanismos de seguridad informática para minimizar posibles riesgos y proteger los activos informáticos de la comisión.

   En este momento la función “N” ha adquirido un papel primordial, tomando como base la justificación explicada en el punto **1.6 “Justificación y Objetivo de la tesis”** del capítulo anterior, aunado a las necesidades actuales y a las fallas anteriormente citadas, cuya principal causa está relacionada con proteger la información en cuanto a sus atributos de confidencialidad, integridad y disponibilidad.

   Por lo tanto, para que la DGI cumpla con la función “N”, se considera necesario implantar un **Sistema de Gestión de la Seguridad de la Información “SGSI”** en la Comisión Nacional de Seguros y Fianzas.

   Entonces el SGSI como parte de la función “N”, requiere de ciertos insumos de la CNSF, de la DGI y de otras dependencias, por lo que la representación del objeto de estudio “DGI”, sería como se muestra en la figura 2.2.

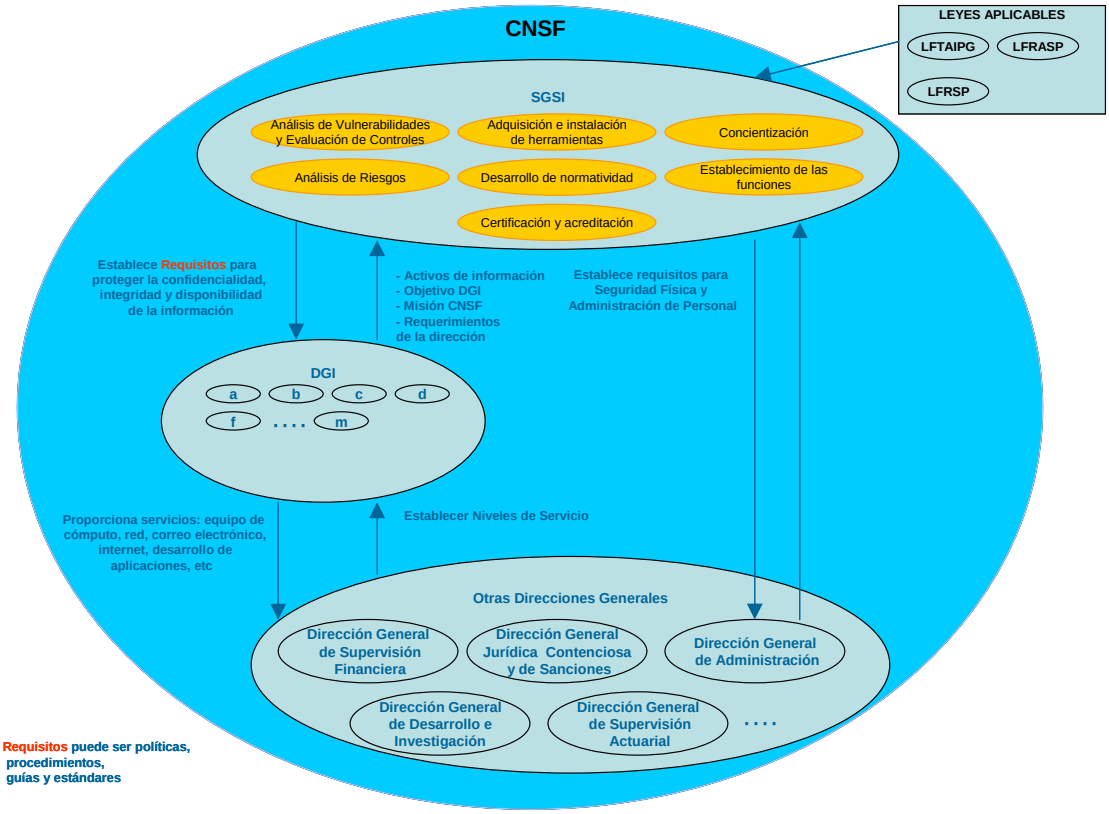


Figura 2.2. Representación del objeto de estudio "DGI"

Si se desea que la implantación de un Sistema de Gestión de la Seguridad de la Información en la Comisión Nacional de Seguros y Fianzas, sea un proceso de conducción[7] (proceso de cambio controlado del objeto conducido), que en este caso la Dirección General de Informática es el objeto conducido, entonces es de suma importancia considerar a la planeación como una actividad primordial que apoya al proceso de conducción.

Este proceso de planeación permitirá visualizar y especificar a la DGI, los objetivos de la conducción y las actividades que permitan realizar el cambio de manera directa, a través de programas y proyectos, que contribuyan al cambio del estado actual al estado deseado.

Para llevar a cabo este proceso de planeación se analizarán dos enfoques: el Diseño Idealizado y la Planeación de Escenarios.

2.2. Planeación de Escenarios[8]

Las empresas buscan su propia forma de persistir, a través de que sean organizaciones flexibles y con una identidad propia. Lo hacen en un mundo en el que el medio ambiente está sujeto a cambios repentinos, que requiere cada vez más una capacidad de entender el medio ambiente en el que se encuentra la organización, estudiar y simular futuros posibles, que permitirán examinar y

[7] O. Gelman y G. Negroe, La Planeación como un proceso básico en la conducción, 1982. P. 257

[8] Gabriel Sánchez Guerrero. Técnicas Participativas de Planeación. (2003) P. 159

seleccionar las estrategias pertinentes de adaptación. Lo cual constituye la práctica principal de la planeación de escenarios.

Hoy puede parecer evidente que el mundo es turbulento o, más exactamente, que requiere reformulación continua y explícita que le den sentido. Aquí es donde la planeación de escenarios y sus procesos asociados se han convertido invaluables, como base para el desarrollo de la nueva estrategia.

Los escenarios son descripciones de futuros admisibles, en los cuales podemos encontrarnos nosotros mismos. Los escenarios son generalmente presentados como un pequeño conjunto de historias acerca de cómo nuestro medio ambiente circundante podría haber evolucionado hacia el futuro. Se producen por un cuidadoso análisis y estructuración de las posibilidades que son relevantes y desafiantes.

De lo anterior, se puede decir que en los procesos de planeación, se le llama escenario a la descripción de una situación futura, unida al grupo de acciones o eventos que deben emprenderse y que permiten el paso de la situación actual hacia la situación futura.

Para la integración de un escenario, ésta se realiza a través de la participación de tres grupos de personas que interactúan de manera continua y estrecha durante el desarrollo de los escenarios: el cliente, el grupo de planeación y los expertos. El grupo de planeación recoge la opinión de los expertos mediante la aplicación de cualquier herramienta participativa de planeación. Con esta información, más las obtenidas de manera directa y del análisis bibliográfico, el grupo de planeación hace uso de modelos de regresión o de simulación para obtener pronósticos y predicciones válidas y confiables.

Finalmente, el escenario se integra redactando de manera global y coherente cómo el sistema o fenómeno en estudio transitaría de un estado actual a un estado posible. Si bien el futuro no está determinado, la construcción de un escenario es un ejercicio valioso que ayuda a comprender y a planear mejores opciones.

En términos generales, el procedimiento para la elaboración de escenarios se realiza en tres grandes etapas: la explicación de la imagen actual e histórica del sistema, el desarrollo de una especie de lógica que permita establecer la relación entre el presente y el futuro y por último, la descripción de la imagen futura, que vendrá siendo propiamente la elaboración de los escenarios que conduzcan al establecimiento de previsiones. Lo anterior se ilustra en la figura 2.3.

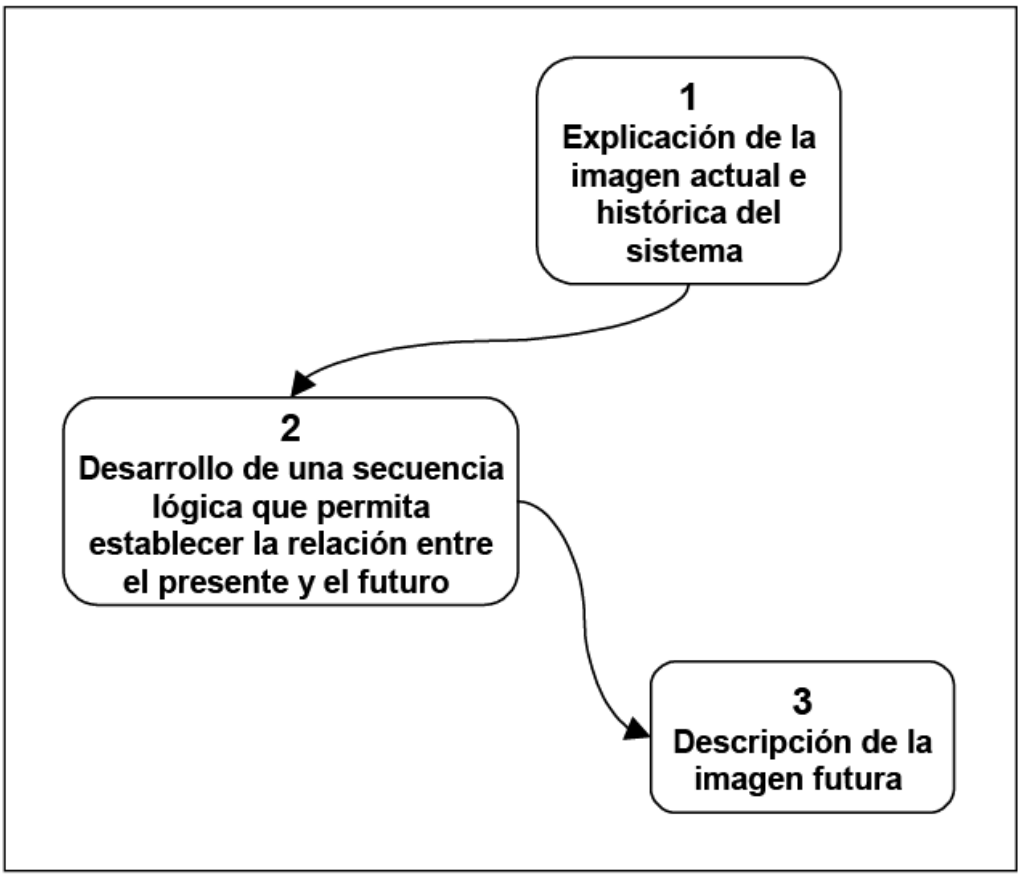


Figura 2.3. Procedimiento para la elaboración de escenarios

[9]A grandes rasgos vemos dos maneras donde los escenarios ayudan a hacer frente a la turbulencia. En primer lugar, ayudan a las partes interesadas "stakeholders" en desarrollar una mejor comprensión sistémica de los orígenes de la turbulencia en su entorno. Ayudando a tener un conocimiento más claro de los elementos predeterminados en su entorno, ayuda a los actores a tener un mejor juicio para reducir la incertidumbre y ésta como puede desempeñarse.

En segundo lugar, los escenarios ayudan en la construcción de un terreno común entre partes interesadas dispares en un entorno turbulento. Les permite centrar su atención colectiva en una serie de futuros alternativos. Los futuros múltiples proporcionan espacio para el surgimiento de supuestos tácitos, que puede ser discutidos y entendidos. El entendimiento de los respectivos puntos de vista sobre cómo el terreno que tienen en común se puede desempeñar en el futuro, permite reunirse a las partes interesadas para alinear y conjuntamente fortalecer su estrategia.

[9] Ramírez Rafael, Selsky John W., Van der Hejden, Kees. Business Planning for Turbulent Times. New Methods for Applying Scenarios. (2008)

2.3. El Diseño Idealizado

[10]El Diseño Idealizado consiste en asumir una actitud interactiva, creando las condiciones y las oportunidades, aprovechando las obstrucciones y reconociendo que las dificultades para intervenir en el futuro son mínimas ante nuestras capacidades creativas para diseñarlo, lo que implica que estaremos poniendo en nuestras manos nuestro futuro o construyendo el futuro deseado a partir de nuestras acciones presentes.

Por esto, es que esta técnica es para aquellos que piensan que el futuro está sujeto a la creatividad y a la voluntad de cambio de las personas.

El Diseño idealizado permite que el proceso de planeación tenga las siguientes características[11]:

- Fomenta la comprensión
  - ✓ No hay mejor manera de comprender algo que diseñarlo.
  - ✓ La manera de abordar más contingencias de las que se pueden planear por separado, es diseñar en la organización o institución suficiente flexibilidad y capacidad de respuesta, para que pueda cambiar rápida y eficazmente.
- Transformar el concepto de viabilidad
  - ✓ El principal obstáculo ante lo que más deseamos somos nosotros mismos. Cuando miramos hacia lo que deseamos desde donde nos encontramos, solemos ver todo tipo de obstáculos impuestos desde fuera. Cuando cambiamos nuestro punto de vista y miramos hacia atrás, hacia el lugar en el que queremos estar, en muchos casos los obstáculos desaparecen.
- Simplifica el proceso de planeación
  - ✓ Se establece un estado desde donde uno quiere estar, reduciendo el número de alternativas que deben considerarse al decidir cómo se va a llegar hasta allí.
- Realza la creatividad, ya que es un proceso en tres etapas
  - ✓ Se identifica una limitación autoimpuesta, un supuesto que realizamos conscientemente o inconscientemente y que limita el número de alternativas que consideramos
  - ✓ Negar o eliminar este supuesto como demasiado restrictivo
  - ✓ Explorar las consecuencias de esta negación

[10] Gabriel Sánchez Guerrero. Técnicas Participativas de Planeación. (2003). P.97

[11] Ackoff, Russell, Planificación de la empresa del futuro, 1983.

- Facilita la implantación (Planeación Participativa)

  ✓ Uno de los principales motivos de que la mayoría de los planes no se implanten por completo es que las personas responsables de hacerlo no tienen la sensación de ser sus propietarios, por lo que el diseño idealizado, sin embargo, requiere de la participación de todos los que se verán afectados por él. Por tanto, la propiedad del plan resultante está muy repartida entre los que deben implantarlo. Esto evita la resistencia. Quienes han participado en su preparación suelen llevar a cabo con entusiasmo la implantación de un diseño y de un plan basado en él.

Ahora las etapas que comprende el Diseño Idealizado, son las que a continuación se explican[12]:

- Idealización

  ✓ Formulación de la problemática

  La Formulación de la problemática, involucra cuatro pasos:

  - Preparar un análisis de sistemas.- Una descripción detallada de cómo opera la empresa.

  - Preparar un análisis de obstrucciones.- Identificar esas características y propiedades de la organización que obstruyen su progreso o resisten su cambio.

  - Preparar proyecciones de referencia.- Describir lo que el futuro de la organización sería si no cambia sus políticas, planes, programas y prácticas o cambia lo que espera en su medio ambiente.

  - Preparar una presentación de la problemática.- Combinar el estado de la organización y sus proyecciones de referencias en un escenario de posibles futuros.

  ✓ Fines de la Planeación

Esta fase de la planeación es el corazón del Diseño Idealizado. Involucra la determinación, por parte de los planeadores, de lo que quisieran que fuera la empresa, si ésta pudiera ser lo que ellos quisieran.

- Realización

  ✓ Medios para la planeación

Las brechas entre el escenario de referencia y el diseño idealizado presentan problemas que requieren una formulación y selección de medios. Un medio es algo que produce un resultado deseado o permite acercarse a él. Los

[12] Ackoff, Russell, Planificación de la empresa del futuro, 1983.

tipos más comunes de medios son: cursos de acción, proyectos, programas y políticas a ser implantadas.

Una vez que se ha formulado un grupo de medios alternativos, se puede elegir uno de ellos. Esta elección siempre está basada en una evaluación comparativa de las alternativas.

✓ Planeación de recursos

Implantar el Diseño Idealizado, requiere de los planeadores identificar y manejar los recursos necesarios, para alcanzar los cambios planeados, incluyendo lo siguiente:

- Determinar cuánto de cada tipo de recurso: personal, económicos, materiales y servicios; facilidades y equipos; e información, conocimiento y entendimiento y deseo se requieren. También se requiere determinar cuándo y dónde aplicar dichos recursos.

- Determinar cuánto de cada recurso estará disponible en el momento y lugar deseados y definir la diferencia entre lo que estará disponible y lo que se requerirá de dichos recursos.

- Determinar que hacer acerca de las diferencias de recursos encontradas.

✓ Implantación y Control

En esta etapa se determinan lo siguientes puntos:

- Cómo monitorear estas asignaciones y programas.

- Cómo ajustar las desviaciones a los programas.

- Cómo monitorear decisiones de planeación para saber si éstas están dando resultado.

Se propone seguir siete factores, que según se ha visto[13], son esenciales para la implantación exitosa de iniciativas que apoyan a la estrategia:

I. Identificación de iniciativas.

Utilizando la nueva estrategia de la compañía como guía, los miembros del equipo de más alto nivel identifican diversas iniciativas potenciales

II. Establecimiento de prioridades entre iniciativas.

[13] Alan P. Brache y Sam Bodle-Scott. Implementación. (2006)

Mediante un proceso de selección, se reducen a proporciones manejables el número de iniciativas candidatas a convertirse en proyectos, a fin de reflejar las más altas prioridades de la organización.

III. Estructura de la organización para la iniciativa

Crear una oficina de proyectos y construir procesos transfuncionales por medio de los cuales se desmantelarán algunos silos funcionales que impedían el éxito de los proyectos.

IV. Cultura para la iniciativa

Una dimensión clave del papel de un alto ejecutivo consiste en definir e instaurar la cultura que apoye mejor a la estrategia.

La cultura es el conjunto de normas, creencias, valores y prácticas prevalecientes que constituyen la personalidad de una organización, entre las características culturales que tienen una influencia particularmente poderosa en la implantación de iniciativas, figuran el grado que se fomenta la innovación, la velocidad con la cual se realizan las operaciones, la voluntad de aceptar riesgos, el modo en que las personas se comunican y el grado en que se ha conferido autoridad para la toma de decisiones a individuos de nivel inferior al del equipo de más alto nivel.

V. Papeles en la iniciativa

Las personas que contribuyen al éxito de los proyectos desempeñan papeles análogos a los que corresponden a los miembros de las organizaciones. Los papeles que con mayor probabilidad deberán desempeñar los integrantes de un proyecto son los que a continuación se detallan.

- El director del programa

  Es el funcionario a cargo de la implantación de estrategias, que se asegura de que todos los proyectos relacionados con el éxito en la implantación de la estrategia de negocios, hayan sido definidos e integrados en un plan de ataque bien enfocado.

- El patrocinador del proyecto

  El patrocinador suele ser extraído de las filas del equipo ejecutivo. Cuando un proyecto tiene un efecto más moderado, se selecciona un gerente de nivel inferior. En cualquier caso, el patrocinador de un proyecto es alguien con “la camiseta bien puesta”, alguien que tiene un interés apasionado en el éxito del proyecto y está dispuesto a respaldar esa pasión con su sentido de responsabilidad.

- El equipo guía y/o el comité de administración de cartera.

Bajo la presidencia del patrocinador, los equipos guía suelen incluir al gerente del proyecto y al jefe de cada uno de los grupos claves que representan a las partes afectadas.

El equipo guía funciona como una junta de directores para la iniciativa, mientras que el comité de administración de cartera es la junta a cargo de todo el conjunto de proyectos. Se asegura que la cartera en su totalidad esté alineada, integrada y comunicada en torno a las estrategias.

- El gerente del proyecto

  Todos los proyectos, pequeños o grandes, a corto o a largo plazo, deben tener un gerente de proyecto que desarrolle el plan de juego y guíe al equipo a la victoria.

- El equipo del proyecto

  Cada uno de los miembros del equipo del proyecto producen o aportan uno o varios de los elementos o “paquetes de trabajo” del proyecto. Sus tareas pueden ser tan diversas como cabildear en el congreso, escribir programas de computación, contratar a los contratistas, negociar préstamos o mover gabinetes de archivo.

  Un equipo eficiente de proyecto contiene no sólo los conocimientos y las habilidades técnicas y la representación funcional adecuados, sino también la mezcla correcta de personalidades, estilos y orientaciones intelectuales

- La población objetivo

  La población objetivo, llamada a menudo “grupos de interés”, la constituyen las personas sobre quienes la iniciativa tendrá algún impacto

  El éxito del proyecto puede requerir también que la población objetivo haga sus propias aportaciones al equipo del proyecto. Esas aportaciones incluyen información, análisis, asesoría técnica, supresión de obstáculos para la implantación, además de sus inquietudes personales.

- Los facilitadores de la gerencia del proyecto

  Los facilitadotes son los expertos en el proceso de administración de proyectos, esos individuos proveen métodos y herramientas y localizan aquellos proyectos que se han salido de curso; en el nivel micro, planean y guían las reuniones del proyecto, desafiando y ampliando la capacidad razonadora del equipo, haciendo el papel de la conciencia acerca de las mejores prácticas de administración para el proyecto, asegurándose de que todos participen, marcando el ritmo y documentando los resultados en el programa de software elegido.

- Software

El software para la administración de proyectos ofrece los mismos beneficios y tiene las mismas limitaciones que otras aplicaciones de software. De la misma manera que el software para procesamiento de textos no redacta por usted las propuestas y el software de hojas de cálculo no toma por usted las decisiones en cuanto al flujo de caja, el software para la administración de proyectos no administra proyectos, es una herramienta valiosa, pero no puede sustituir el buen juicio humano.

VI. Proceso de administración de la iniciativa

Se requiere un enfoque sólido y amigable con el usuario para la administración de iniciativas; se necesita consistencia en el modo de pensar de las personas en materia de proyectos. Por medio de implantar una metodología, un proceso, un protocolo, una plantilla o un juego de herramientas que obliguen a utilizar un idioma en común entre las personas.

El idioma es el principio organizador del pensamiento y constituye la estructura para el discurso. Si una organización aborda sus mayores desafíos con un idioma y un enfoque común, aumentará sus probabilidades de éxito para la implantación de estrategias.

Existe una reserva oficial de normas y prácticas que puede ayudar a establecer ese enfoque para la administración de iniciativas, que se identifica como el Cuerpo de Conocimientos de la Gerencia de Proyectos, conocido comúnmente como el PMBOK[14].

VII. Información y monitoreo de iniciativas

Para alcanzar un buen monitoreo y control se recomienda realizarlo sobre las siguientes dimensiones:

- Los proyectos o iniciativas.- Son actividades interdependientes, no repetitivas, dirigidas hacia una meta.

- Los programas.- Son un conjunto de proyectos que tienen una meta en común.

- La cartera.- Es todo el conjunto de programas y proyectos

- El proceso.- Es la secuencia de actividades y protocolos por medio de los cuales identifica los proyectos, los aprueba, los planea, los dota de personal, los implanta y los administra.

Para el diseño de un sistema de monitoreo y control, se deben seguir los principios:

[14] Project Management Institute Publications, A Guide to the Project Management Body of Knowlegde: Fourth Edition: 2009

- La calidad de los informes que se reciba acerca de las principales áreas: programas críticos para la misión, la cartera general y la implantación de estrategias; sólo puede ser tan buena como la calidad de la información que reciba sobre los proyectos individuales.

- Toda la información sobre proyectos y programas debe presentarse en un formato que muestre el estado deseable en contra del estado real, que ponga de relieve la magnitud de cualesquiera desviaciones positivas o negativas.

- Mostrar comparaciones entre la situación en este mes o trimestre con el mes o trimestre anterior para todas las dimensiones claves, lo cual permitirá que se detecte cualquier tendencia.

Por otra parte, para dar información acerca de las iniciativas se deben considerar los siguientes elementos:

- Resultados que debe producir la iniciativa.

- El tiempo en el cual dichos resultados se habrán logrado

- La máxima inversión que se requerirá para producir esos resultados

- La solución de problemas

- La satisfacción de los grupos de interés

2.4. El proceso de planeación para la implantación del Sistema de Gestión de la Seguridad de la Información

Basándose en las características presentadas entre la Planeación de Escenarios y el Diseño Idealizado, el proceso de planeación para la implantación del SGSI en la Comisión Nacional de Seguros y Fianzas, se basará en el Diseño Idealizado, por las siguientes razones:[15] [16]

- La planeación de escenarios es la visualización de los futuros posibles de acuerdo a lo que tenemos actualmente y a los conductores detectados en el medio ambiente, mientras que en el diseño idealizado se produce un futuro deseado que será aproximado gradualmente

  Esta propiedad del Diseño idealizado, como se analizó anteriormente, permitirá simplificar el proceso de planeación, ya que desde un principio establece un estado desde donde uno quiere estar, reduciendo el número de alternativas que deben considerarse al decidir cómo se va a llegar hasta allí.

- La planeación de escenarios se centra en un actor, por ejemplo, un ejecutivo, un responsable político o una empresa; con el objetivo de ayudar a este actor a

[15] Ramírez Rafael, Selsky John W., Van der Hejden, Kees. Business Planning for Turbulent Times. New Methods for Applying Scenarios. (2008)

[16] Ackoff, Russell. Planificación de la empresa del futuro. (1983)

enfrentar de una manera óptima las turbulencias que afronta, mientras que el Diseño Idealizado se centra en un tema de discusión, sobre el cual las diferentes partes interesadas tratan de encontrar un terreno común, sobre el cual construir un futuro deseado.

Más aún, la planeación de escenarios puede ser pensado como un conjunto de proyecciones de referencia de lo que puede suceder en el futuro, mientras que el producto de un diseño idealizado es, por un lado, la imagen de un futuro deseado por todos las partes interesadas y, por otro, un conjunto de cursos de acción que todas las partes interesadas llevarán a cabo para abordar el futuro deseado.

Estas propiedades citadas del Diseño Idealizado se desarrollan, ya que éste enfoque utiliza la planeación participativa, explicada anteriormente, la cual permite que la pertenencia del plan resultante esté muy repartida entre los que deben implantarlo, evitando la resistencia. Adicionalmente, quienes han participado en su preparación suelen llevar a cabo con entusiasmo la implantación de un diseño y de un plan basado en él.

De tal manera, para que la implantación del SGSI este conforme al Diseño Idealizado, se desarrollarán los capítulos de este trabajo conforme a las etapas descritas en la sección anterior.

- Formulación de la problemática **(Capítulo 1)**

  - ✓ Fines de la Planeación **(Capítulo 2)**

  - ✓ Medios para la planeación **(Capítulo 3)**

  - ✓ Planeación de recursos **(Capítulo 4)**

  - ✓ Implantación y Control **(Capítulo 5)**

2.5. Determinación de los Fines de la Planeación

Conforme a lo explicado en la sección anterior con respecto al enfoque del diseño idealizado, el siguiente paso es determinar lo que quisieran que fuera la empresa si ésta pudiera ser lo que quisieran, a través de establecer los ideales, objetivos y metas, a partir de la misión que debe cumplir la empresa.

Como se mencionó la **misión de la Comisión Nacional de Seguros y Fianzas es la siguiente:**

“La CNSF es un organismo desconcentrado de la SHCP (Secretaría de Hacienda y Crédito Público) el cuál tiene como misión el de supervisar de

manera eficiente, que la operación de los sectores asegurador y afianzador se apeguen al marco normativo, preservando la solvencia y estabilidad financiera de las instituciones, para garantizar los intereses del público usuario, así como promover el sano desarrollo de estos sectores con el propósito de extender la cobertura de sus servicios a la mayor parte posible de la población."

Basándose en esta misión y en el papel primordial que la función "N" de la Dirección General de Informática ha adquirido, a consecuencia de las necesidades actuales y a las fallas anteriormente descritas, se establece el siguiente ideal:

Ideal

- Diseñar e implantar una solución integral de seguridad de la información, para lograr el aseguramiento de sus procesos de negocio e incrementar la confiabilidad en su operación de la CNSF.

Para alcanzar este ideal, se establecen los siguientes objetivos:

Objetivos de TI

- Asegurar que los servicios de TI están disponibles según se requieran.
- Asegurar un mínimo impacto al negocio en caso de una interrupción o cambio en los servicios de TI.
- Asegurar que los servicios y la infraestructura de TI pueden resistir y recuperarse de fallas originadas por un error, ataque deliberado o desastre.
- Garantizar que la información crítica y confidencial esté prohibida a aquellos que no tienen acceso a ella.
- Garantizar que las transacciones e intercambios de información automatizados del negocio sean confiables.
- Mantener la integridad de la información y de la infraestructura de procesamiento.
- Proteger y mantener registro de todos los activos de TI.

Por último, para cumplir con estos objetivos se establecen las metas correspondientes:

Metas de Proceso

- Establecer un plan de continuidad de TI que soporte los planes de continuidad del negocio.
- Desarrollar planes de continuidad de TI que puedan ejecutarse, probarse y mantenerse.
- Minimizar la posibilidad de interrupción de los servicios de TI.
- Permitir el acceso a información crítica y sensible solo a usuarios autorizados.
- Identificar, monitorear y reportar vulnerabilidades e incidentes de seguridad.
- Detectar y resolver accesos no autorizados a la información, aplicaciones e infraestructura.
- Minimizar el impacto de las vulnerabilidades y de los incidentes de

seguridad.

Metas de Actividades

- Desarrollar y mantener (mejorar) los planes de contingencia de TI
- Capacitación y pruebas de los planes de contingencia
- Almacenamiento de copias de los planes de contingencia fuera de las instalaciones
- Entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad.
- Administración de las identidades y autorizaciones de los usuarios de manera estándar.
- Definición de incidentes de seguridad.
- Pruebas de seguridad regulares.

Capítulo 3. Medios de la Planeación

En este capítulo, se evaluarán tres alternativas que representan estándares internacionales o marcos de referencia para implantar un Sistema de Gestión de la Seguridad de la Información, lo que permitirá posteriormente alinear los programas y proyectos necesarios para la implantación del SGSI, con los requisitos que establezca el estándar internacional seleccionado.

3.1 Formulación de Medios (Alternativas)

La implantación de un SGSI pretende disolver la problemática presentada, a través de cerrar las brechas entre los escenarios de referencia y el diseño idealizado, ambos anteriormente citados.

Para cerrar esta brecha, es necesario formular los medios, que consiste en establecer los programas y proyectos para la implantación del SGSI, los cuales deben estar alineados a los requisitos que establezca algún estándar de seguridad internacional, lo cual equivale a ajustarse a un marco de referencia, que permita adoptar los procesos, procedimientos, actividades, entregables y roles que deberá considerar el SGSI de la Comisión Nacional de Seguros y Fianzas.

Por lo que, para este trabajo se analizarán los siguientes estándares de seguridad:

- Control Objectives for Information and related Technology **(**COBIT)
- **I**nformation **T**echnology **I**nfrastructure **L**ibrary (ITIL)
- ISO 27001

Control Objectives for Information and related Technology **(COBIT)**[17]

COBIT es el acrónimo de Control Objectives for Information and related Technology cuya traducción al español es, Objetivos de Control para la Información y Tecnologías relacionadas.

COBIT es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información, (ISACA, en inglés: Information Systems Audit and Control Association), y el Instituto de Administración de las Tecnologías de la Información (ITGI, en inglés: IT Governance Institute) en 1992.

CobiT se estructura en cuatro partes; la principal de ellas se divide de acuerdo con 34 procesos de TI. Cada proceso se cubre en cuatro secciones (objetivo de control de alto nivel para el proceso, los objetivos de control detallados, directrices de gestión y el modelo de madurez para el objetivo) que dan una visión completa de cómo controlar, gestionar y medir el proceso. Utiliza un ciclo de vida de tipo PDCA que lo integra en los procesos de negocio.

Lo anterior, se muestra en la figura 3.1.

[17] COBIT® 4.1 (2005)

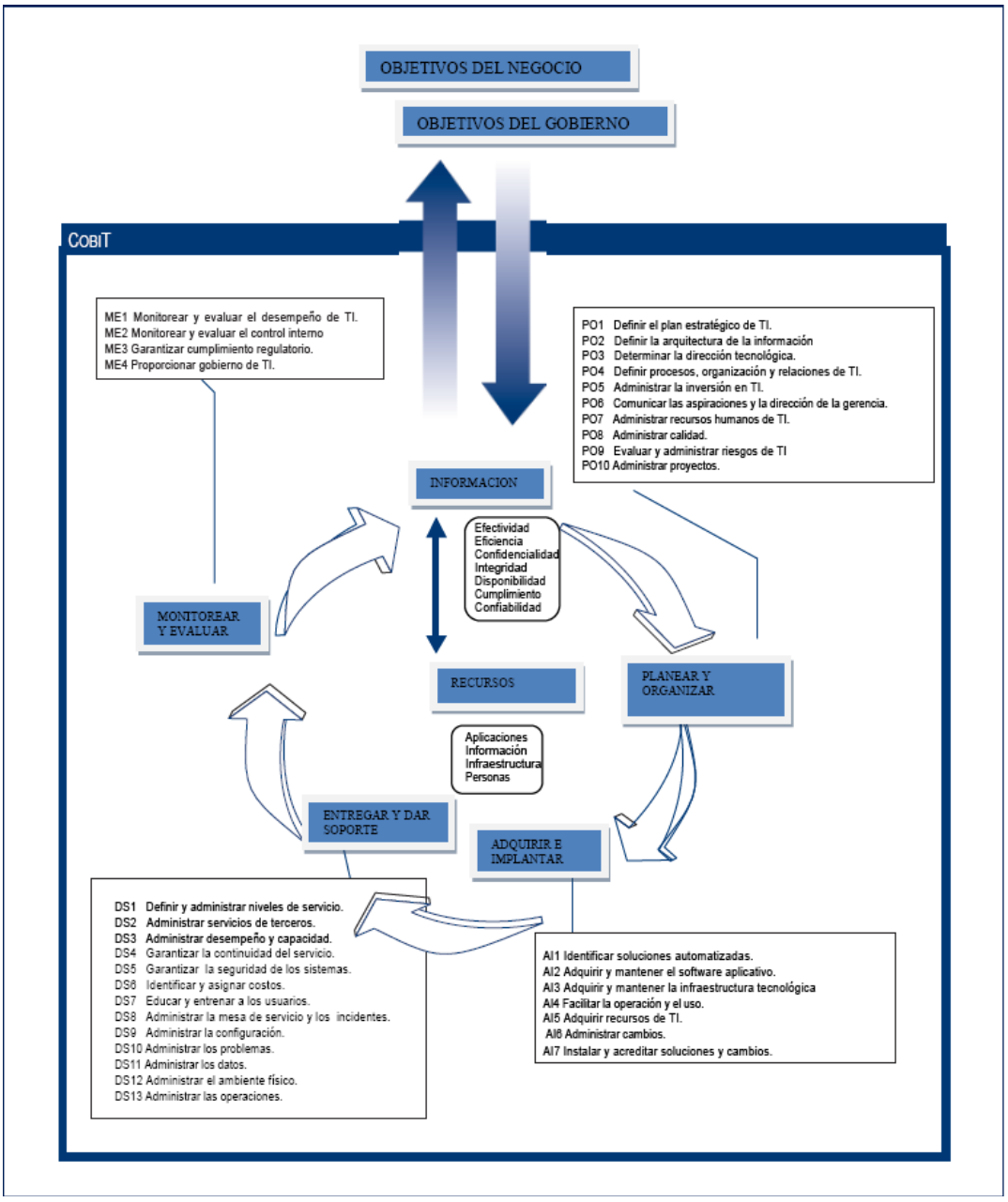


Figura 3.1. Procesos de CobiT

Information **T**echnology **I**nfrastructure **L**ibrary **(ITIL)** [18]

ITIL es el acrónimo de **I**nformation **T**echnology **I**nfrastructure **L**ibrary cuya traducción al español es, Biblioteca de Infraestructura de Tecnologías de Información.

[18] ITIL® 1.1 (2001)

ITIL es un marco de trabajo de las mejores prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI.

Las áreas cubiertas por ITIL en cada documento publicado por la OGC son:

- Soporte al servicio: asegurar que el cliente (externo o interno) recibe adecuadamente un servicio, que es gestionado además de la mejor forma posible.
- Entrega del servicio: administración de los servicios de soporte y mantenimiento que se prestan al cliente.
- Planificación de la implantación: determina las ventajas de implantar ITIL en una determinada organización.
- Administración de aplicaciones: conjunto de buenas prácticas para la gestión de todo el ciclo de vida de las aplicaciones, centrándose sobre todo en definición de requisitos e implantación de soluciones.
- Administración de la infraestructura de tecnologías de la información y
- comunicaciones: gestión de la administración de sistemas como máquinas, redes o sistemas operativos, entre otros.
- Administración de seguridad: proceso para la implantación de requerimientos de seguridad; relaciona las áreas ITIL de soporte y entrega de servicio.
- Administración de activos de software: pautas necesarias para la gestión del software adquirido y/o de desarrollo propio.
- Entrega de servicios desde un punto de vista de negocio: clientes fieles, servicios de externalización y gestión del cambio, entre otros.

En la figura 3.2, se muestran las áreas cubiertas por ITIL.

Figura 3.2. Las áreas cubiertas por ITIL

ISO27001[19]

ISO27001 es muy diferente entre COBIT e ITIL, porque ISO27001 es un estándar de seguridad, así que tiene menos dominios pero son más profundos con respecto a crear sistemas de gestión de la seguridad de la información.

ISO 27001 está agrupado en 11 capítulos (dominios de control), los cuáles contienen una serie de controles, que constituyen objetivos más específicos relacionados con el dominio correspondiente.

1. Política de Seguridad
2. Seguridad Organizacional
3. Manejo de Activos de Información
4. Seguridad en Recursos Humanos
5. Seguridad física
6. Manejo de comunicaciones y operaciones
7. Control de acceso
8. Adquisición, desarrollo y mantenimiento de sistemas de información
9. Manejo de incidentes de seguridad.
10. Gestión de continuidad de operaciones
11. Cumplimiento con legislaciones

3.2 Evaluación de Medios (Alternativas)

Una vez que se formuló un grupo de medios alternativos, se puede elegir uno

[19] ISO 27001® (2008)

de ellos. Esta elección se basará en una evaluación comparativa con base en los siguientes criterios:

- Si la alternativa es un “Estándar internacional”
- Si la alternativa está enfocado principalmente a la seguridad de la información
- Si la alternativa produce un Sistema de Gestión de la Seguridad de la Información que se puede certificar

En la tabla 3.1. se muestra un análisis comparativo entre estas tres alternativas:

CRITERIO/ ALTERNATIVA	COBIT	ITIL	ISO27001
Estándar Internacional	SI	SI	SI
Enfocado principalmente a la seguridad de la información	NO	NO	SI
Se puede certificar el SGSI	NO	NO	SI

Tablas 3.1. Comparativo de las alternativas para implantar el SGSI

Derivado del análisis comparativo, se determina que ISO27001 es la alternativa que servirá de referencia para implantar el SGSI de la Comisión Nacional de Seguros y Fianzas, ya que es la única alternativa que es un estándar internacional y está enfocada principalmente en crear “Sistemas de Gestión de la Seguridad de la Información” que se pueden certificar por una entidad externa a la organización.

Adicionalmente a lo anterior, se tienen diversos beneficios que se han expuesto en las conferencias sobre seguridad de la información al utilizar ISO27001, entre los que destacan:

- Obtener un certificado por parte de un tercero, demuestra que la organización ha direccionado, implantado y controlado la seguridad de la información
- Accionistas, clientes y socios estarán conformes, en el entendido de que la administración de la información y de los sistemas es segura.
- Demuestra credibilidad y confianza.
- Puede llevar a ahorros en costos de operación. Aún con una simple brecha de seguridad puede causar costos significantes a la empresa.
- Establece aquellas regulaciones y leyes relevantes que deben cumplirse.
- Asegura que el compromiso hacia la seguridad de la información exista en todos los niveles a través de la organización.

3.3 Establecimiento de programas y proyectos

El siguiente paso es establecer los programas y proyectos que permitirán llevar a la CNSF del estado actual al estado idealizado previamente establecido en el

capítulo II, el cual corresponde a: “Diseñar e implantar una solución integral de seguridad de la información, para lograr el aseguramiento de los procesos de negocio e incrementar la confiabilidad en su operación de la CNSF”.

Derivado que se eligió la norma internacional ISO 27001, como un marco de referencia para la implantación del Sistema de Gestión de la Seguridad de la Información en la CNSF, los programas y proyectos también deberán estar alineados con los requisitos que establece esta norma.

Los programas y proyectos que ayudarán a cumplir con lo anterior, son los que se muestran en la tabla 3.2.[20]

Programa I. Planeación y organización.

Programa II. Análisis de Vulnerabilidades y Evaluación de Controles.

- Proyecto I.- Identificación de Aplicaciones Críticas
- Proyecto II. Identificación del Árbol de Activos
- Proyecto III.- Análisis de Vulnerabilidades
- Proyecto IV.- Evaluación de Controles
- Proyecto V.- Diagnóstico de Concientización (Awareness)
- Proyecto VI.- Clasificación y Ponderación de Vulnerabilidades
- Proyecto VII. Recomendación para corregir las Vulnerabilidades

Programa III. Análisis de Riesgos.

Programa IV. Adquisición e instalación de herramientas.

Programa V. Desarrollo de Normatividad.

- Proyecto I.- Desarrollo de Políticas, Estándares y Guías
- Proyecto II.- Desarrollo de Procedimientos

Programa VI. Establecimiento de la Función de Seguridad.

- Proyecto I.- Diagnóstico de la Organización y de las funciones vigentes
- Proyecto II.- Preparación y concertación de responsables de Seguridad en TI
- Proyecto III.- Preparación y entrega de Resultados

Programa VII. Concientización (Awareness).

- Proyecto I.- Plan de Concientización

[20] Comisión Nacional de Seguros y Fianzas. INVITACION DE CARÁCTER NACIONAL A CUANDO MENOS TRES PERSONAS INV/008/07. (2007)

- Proyecto II.- Ejecución del Plan de Concientización

Programa VIII. Certificación y Acreditación.

- Proyecto I.- Definición
- Proyecto II.- Verificación
- Proyecto III.-Validación
- Proyecto IV. Post-Acreditación

Programa IX. Cierre.

Tabla 3.2. Programas y proyectos para la implantación del SGSI en la CNSF

3.4 Detalle de los Programas y Proyectos del Sistema de Gestión de la Seguridad de la Información en la Comisión Nacional de Seguros y Fianzas

Cada uno de los programas y proyectos que servirán para la implantación del Sistema de Gestión de la Seguridad de la Información en la Comisión Nacional de Seguros y Fianzas, tendrán los siguientes elementos: objetivo, alcance, actividades y entregables.

PROGRAMA I. PLANEACIÓN Y ORGANIZACIÓN

En este programa se deberán afinar y precisar los objetivos y alcances antes de comenzar el trabajo, generando también la capacidad de establecer las actividades detalladas necesarias que ayuden a lograr estos objetivos.

Adicionalmente, la organización deberá definir de forma clara los roles y responsabilidades que tomará cada integrante a través de un documento de equipo de proyecto, siendo esto de vital importancia en la integración de equipos interdisciplinarios con actividades distintas y objetivos comunes.

OBJETIVO

Formalizar la planeación y definir los alcances detallados de cada uno de los proyectos, así como recolectar la información necesaria para identificar de forma precisa los alcances.

ALCANCE

La planeación deberá considerar las actividades necesarias para llevar el control y seguimiento de las actividades y entregables de cada uno de los programas y proyectos.

ACTIVIDADES

Formalizar la planeación de trabajo para cada uno de los programas y proyectos:

- Afinar el alcance.
- Desarrollar, afinar y aprobar el plan de trabajo.
- Definir y desarrollar el documento con la organización, roles y responsabilidades del equipo que participará.

ENTREGABLES

- Plan detallado de trabajo de cada uno de los programas y proyectos.
- Reunión de inicio de proyecto (“Kick-off”).
- Organización del plan, organigrama y asignación de roles y responsabilidades (Project Charter).
- Reporte del Análisis del Valor Ganado generado semanalmente

PROGRAMA II. ANÁLISIS DE VULNERABILIDADES Y EVALUACIÓN DE CONTROLES

Se deberán identificar todas aquellas debilidades de seguridad en la tecnología de información de la organización que se llevará a cabo mediante revisiones de cumplimiento contra mejores prácticas internacionales ISO/IEC 17799:2005, así como identificar aquellos controles necesarios para mantener cierto grado de seguridad.

PROYECTO I. IDENTIFICACIÓN DE APLICACIONES CRÍTICAS

OBJETIVO

Identificar y priorizar las aplicaciones de negocio.

ALCANCE

Todas las aplicaciones de negocio de la Comisión Nacional de Seguros y Fianzas.

ACTIVIDADES

- Definir el enfoque de la sesión.
- Seleccionar la audiencia considerando a la gente de negocio.
- Definir el propósito de la sesión de la información.
- Determinar los recursos necesarios para lograr los objetivos de identificación y priorización de los procesos críticos.
- Realizar la sesión.
- Realizar el consenso y obtener los resultados.
- Analizar los resultados de la sesión.
- Realizar el reporte de resultados.

ENTREGABLES

- Informe de las aplicaciones críticas de negocio.

PROYECTO II. IDENTIFICACIÓN DEL ÁRBOL DE ACTIVOS

OBJETIVO

Realizar la identificación de activos que soportan las aplicaciones críticas de negocio.

ALCANCE

Activos de las capas Física, Red, Sistema Operativo, Base de Datos y Aplicaciones.

ACTIVIDADES

- Realizar la identificación de los componentes tecnológicos de las capas de datos, sistema operativo, red y física que soportan las aplicaciones críticas de negocio.
- Definir el árbol de activos, asegurando la interdependencia que hay entre cada capa y componente.

ENTREGABLES

- Reporte de Árbol de Activos.

PROYECTO III. ANÁLISIS DE VULNERABILIDADES

El análisis de vulnerabilidades deberá comprender la revisión de las capas de red y sistemas operativos y bases de datos. Esta revisión se llevará a cabo mediante el uso de herramientas especializadas, las cuales se encargarán de la identificación de vulnerabilidades de seguridad existentes en la infraestructura tecnológica que soporta las aplicaciones críticas de la Comisión Nacional de Seguros y Fianzas.

Las herramientas de identificación de vulnerabilidades se configurarán en su nivel de revisión más estricto, con la finalidad de profundizar y fortalecer la revisión de las vulnerabilidades. Estas herramientas no deberán representar ningún riesgo para la seguridad de los equipos e información, como pueden ser ataques de negación de servicios (DoS: Denial of Service), códigos maliciosos, caballos de Troya, saturación de memoria, saturación de discos, etc.

III.1. ANÁLISIS DE VULNERABILIDADES DE RED "DESDE EL EXTERIOR"

En el enfoque "desde el exterior" los trabajos de vulnerabilidades serán realizados fuera de las instalaciones y redes de la CNSF, en el cual se utilizará Internet como infraestructura de trabajo. En este enfoque no se requerirán cuentas de acceso ni información adicional que pudiera ser utilizada para la evaluación.

OBJETIVO

Realizar la identificación y el análisis de las vulnerabilidades existentes en la infraestructura de red de la CNSF considerando un enfoque "desde el exterior".

ALCANCE

Análisis de vulnerabilidades sobre los componentes del segmento externo de red de la CNSF.

ACTIVIDADES

Las actividades generales para el análisis de vulnerabilidades "desde el exterior" son:

- Identificar los recursos conectados a Internet.
- Realizar el escaneo de puertos y servicios de red.
- Instalar y configurar las herramientas comerciales y de uso público en el equipo.
- Realizar la recopilación y el estudio de las vulnerabilidades identificadas.
- Ejecutar pruebas de intrusión y obtener evidencias de intrusiones exitosas.
- Realizar el análisis y el informe de las vulnerabilidades identificadas, así como las alternativas de solución.

ENTREGABLES

- Informe de análisis de vulnerabilidades.
- Reportes detallados de identificación de vulnerabilidades y alternativas técnicas de solución.

III.2. ANÁLISIS DE VULNERABILIDADES DE RED "DESDE EL INTERIOR"

El análisis de vulnerabilidades de red se llevará a cabo mediante la revisión de aquellos equipos que se encuentran dentro de la red interna, en donde se conectará a la red como un usuario más, identificando así aquellas vulnerabilidades que pueden ser explotadas por cualquier usuario de red dentro de la institución.

OBJETIVO

Realizar la identificación y el análisis de las vulnerabilidades existentes en la infraestructura de red.

ALCANCE

Este análisis se aplicará a los segmentos de red identificados dentro del proyecto "Identificación del árbol de activos".

ACTIVIDADES

Las actividades a realizar para la identificación de vulnerabilidades dentro de la red son:

- Definición de los parámetros de configuración de las herramientas.
- Calendarización de la ejecución de las herramientas.
- Instalación y configuración de las herramientas.
- Realizar la identificación de vulnerabilidades en la red siendo algunos posibles puntos de revisión, con carácter enunciativo, más no limitativo, como se muestra en la tabla 3.3.

✓ Análisis de vulnerabilidades en la configuración del DNS.	✓ Obtener acceso a recursos de red de Windows y Unix.
✓ Análisis de vulnerabilidades de NetBIOS.	✓ Descubrir vulnerabilidades adicionales.
✓ Identificación de recursos de red.	✓ Descubrir servicios RPC.
✓ Enumeración de objetivos de red.	✓ Obtener mapas de servidores NIS.
	✓ Descubrir vulnerabilidades SMB.

- ✓ Escaneo de recursos de red utilizando el protocolo ICMP.
- ✓ Descubrir recursos de red.
- ✓ Descubrir servicios seleccionados de TCP.
- ✓ Obtener banners de los servicios TCP.
- ✓ Descubrir vulnerabilidades NFS.
- ✓ Utilizar Windows networking para descubrir vulnerabilidades.
- ✓ Descubrir vulnerabilidades de los recursos de red de NetWare.
- ✓ Obtener acceso a través del servidor de login.
- ✓ Descubrir vulnerabilidades SMP.
- ✓ Descubrir vulnerabilidades FTP.
- ✓ Descubrir vulnerabilidades IRC.
- ✓ Descubrir vulnerabilidades HTTP.
- ✓ Descubrir vulnerabilidades Finger.
- ✓ Descubrir servicios seleccionados de TCP y UDP.
- ✓ Descubrir vulnerabilidades en agentes SNMP identificados.
- ✓ Adivinar nombres comunitarios de SNMP.

Tabla 3.3. Posibles puntos de revisión en la identificación de vulnerabilidades

- Realizar el análisis y el informe de las vulnerabilidades identificadas, así como las alternativas de solución.

ENTREGABLES

- Scripts o programas con los resultados obtenidos de las pruebas.
- Reporte de vulnerabilidades de red arrojado por las herramientas.
- Informe de análisis de vulnerabilidades de red.
- Reportes detallados de identificación de vulnerabilidades de red y alternativas de solución, que contenga al menos la siguiente información.
    - ✓ Nombre de la vulnerabilidad.
    - ✓ Descripción.
    - ✓ Solución.
    - ✓ Direcciones IP afectadas.

III.3. ANÁLISIS DE VULNERABILIDADES DE SISTEMA OPERATIVO

El análisis de vulnerabilidades a sistemas operativos se llevará a cabo mediante la instalación de herramientas automatizadas o en su caso en la aplicación de mejores prácticas, las cuales se basan en la revisión de estándares de seguridad de cumplimiento, con la finalidad de encontrar vulnerabilidades dentro de los equipos a revisar.

OBJETIVO

Realizar la identificación y el análisis de vulnerabilidades existentes en los servidores que soportan las aplicaciones críticas de la Comisión Nacional de Seguros y Fianzas.

ALCANCE

Análisis de vulnerabilidades sobre los servidores que soportan las aplicaciones críticas de negocio.

ACTIVIDADES

Las actividades a realizar para la identificación de vulnerabilidades de los servidores son:

- Definición y análisis de los parámetros de configuración de las herramientas.
- Calendarización de la ejecución de las herramientas.
- Instalación y configuración de las herramientas.
- Realizar la identificación de vulnerabilidades mediante la ejecución de herramientas, configurando parámetros de revisión alineados con el ISO/IEC 17799:2005.
- Los equipos no deberán ser apagados o reiniciados antes, durante o después del análisis de vulnerabilidades.
- Realizar el análisis y el informe de las vulnerabilidades identificadas, así como las alternativas de solución.

ENTREGABLES

- Reporte de vulnerabilidades de S.O. agrupados con respecto al ISO/IEC 17799:2005.
- Informe de análisis de vulnerabilidades de S.O.
- Reportes detallados de identificación de vulnerabilidades de S.O. y alternativas de solución, que contenga por lo menos la siguiente información:
    - ✓ Nombre de la vulnerabilidad.
    - ✓ Descripción.
    - ✓ Solución.

III.4. ANÁLISIS DE VULNERABILIDADES DE BASES DE DATOS

El análisis de vulnerabilidades se llevará a cabo dependiendo del tipo de base de datos a revisar, debido a la especialización y tipo de herramienta que se requiere para cada tipo de base de datos, pero en cualquier análisis se deberá garantizar la no afectación del desempeño de la base datos y del servidor en donde esta radica.

Cabe señalar que en caso que no exista una herramienta ad hoc que identifique de manera automatizada las vulnerabilidades existentes en la Base de Datos, la revisión se llevará de manera manual, utilizando estándares internacionales de seguridad y mejores prácticas del mercado.

OBJETIVO

Identificar las vulnerabilidades existentes dentro de las bases de datos que soportan las aplicaciones críticas de la Comisión Nacional de Seguros y Fianzas.

ALCANCE

Base de Datos utilizadas por las aplicaciones identificadas en el árbol de activos de la CNSF.

ACTIVIDADES

Forma Automatizada (haciendo uso de una herramienta)

- Instalar la herramienta de revisión de Base de Datos.
- Actualizar la herramienta de revisión de Base de Datos para que pueda llevar a cabo la identificación de las vulnerabilidades más nuevas.
- Configurar la herramienta de revisión de vulnerabilidades de Base de Datos.
- Ejecutar la herramienta de revisión de vulnerabilidades de Base de Datos.
- Obtener y analizar los resultados arrojados por la herramienta.

Forma Manual (mediante el uso de guías de revisión), en caso de no poder llevarse a cabo la revisión automatizada.

- Identificar los controles existentes respecto a la administración de seguridad en Bases de datos.
- Evaluar el cumplimiento de los controles identificados con las prácticas de seguridad generalmente aceptadas:

  - ✓ Políticas de control de acceso.
  - ✓ Utilización de la base de datos.
  - ✓ Monitoreo del acceso y uso de la base de datos.
  - ✓ Actualización y control de versiones.
  - ✓ Procedimientos de control de cambios.
  - ✓ Control de respaldos y recuperaciones.
  - ✓ Segregación de funciones (DBMS), etc.

ENTREGABLES

- Reporte de Vulnerabilidades arrojado por la herramienta.
- Informe detallado de vulnerabilidades junto con su esquema de solución, que al menos contenga la siguiente información:
  - ✓ Nombre de la vulnerabilidad.
  - ✓ Descripción.
  - ✓ Solución.
- Informe de evaluación de controles de administración de seguridad.

PROYECTO IV. EVALUACIÓN DE CONTROLES

En el enfoque de evaluación de controles comprende el análisis de vulnerabilidades, en este caso son aquellas que se obtienen mediante la revisión de controles de seguridad alineados con estándares internacionales tales como ISO/IEC 17799:2005, COBIT, NIST, entre otros.

IV.1. REVISIÓN DE CONTROLES DE SEGURIDAD A APLICACIONES

La revisión de la existencia y cumplimiento de controles de seguridad se deberá realizar en las aplicaciones críticas de negocio identificadas, dentro de los cuales pueden cubrirse:

- ✓ Control de Cambios a la aplicación
- ✓ Controles de accesos

- ✓ Respaldos
- ✓ Segregación de funciones, etc.

Este tipo de revisión se deberá llevar a cabo haciendo uso de las mejores prácticas internacionales para la revisión de controles de aplicación, emitidos por la ISACA (Information System Audit. and Control Association) y por instituciones reconocidas en la materia.

OBJETIVO

Evaluar los controles de aplicación diseñados e implementados en las aplicaciones críticas de negocio.

ALCANCE

Aplicaciones críticas de negocio.

ACTIVIDADES

- Identificar los controles existentes respecto a la administración de seguridad en aplicaciones.
- Realizar entrevistas de trabajo y visitas de campo para la evaluación de controles de aplicación.
- Evaluar el cumplimiento de los controles identificados con las prácticas de seguridad generalmente aceptadas:
  - ✓ Políticas de control de acceso.
  - ✓ Utilización de la aplicación.
  - ✓ Respaldos de información.
  - ✓ Control de cambios,
  - ✓ Procesos en lote, etc.

ENTREGABLES

- Informe de evaluación de controles de aplicación.

IV.2. REVISIÓN DE CONTROLES CAPA FÍSICA (CENTRO DE CÓMPUTO PRINCIPAL)

La revisión de controles de seguridad a la capa física se deberá realizar verificando la existencia y cumplimiento de aspectos tales como:

- ✓ Controles de accesos físico (guardias, cerraduras, puertas, etc.).
- ✓ Sistemas de supresión de incendio.
- ✓ Controles ambientales (aire acondicionado).
- ✓ Energía eléctrica (UPS, plantas de emergencia), etc.

Estas revisiones se llevan a cabo mediante la aplicación de cuestionarios y entrevistas alineados con estándares internacionales tales como ISO/IEC 17799:2005, COBIT, NIST, Best Practices, entre otros.

OBJETIVO

Evaluar los controles de TI que satisfagan los requerimientos de proveer una seguridad física adecuada, que proteja los componentes de TI de eventos humanos y naturales en las instalaciones del centro de cómputo de la Comisión Nacional de Seguros y Fianzas.

ALCANCE

Controles existentes sobre los componentes identificados en el árbol de activos relacionados con la capa física.

ACTIVIDADES

- Identificación de centros de cómputo sobre en los que se ubican los componentes físicos identificados en el árbol de activos.
- Revisión para cada tipo de sistema de control y protección (Operativa de las Instalaciones, Técnica de las herramientas y sistemas; herramientas, equipos de Seguridad y Protección; Medio Ambiente (Energía Eléctrica, Aire, Agua, Detección de movimiento, Fuego, Temperatura/Humedad, etc.).
- Verificar la existencia de planes de recuperación de desastres (DRP) y verificación del plan de pruebas.
- Revisar el cumplimiento con requerimientos externos, aspectos legales, seguros, licencias, acuerdos de niveles de servicio, contratos de servicio con proveedores y terceros.
- Visitas guiadas al centro de computo

ENTREGABLES

- Informe de evaluación de controles de administración de seguridad física para el centro de cómputo.

PROYECTO V. DIAGNÓSTICO DE CONCIENTIZACIÓN (AWARENESS)

El Diagnóstico de Concientización deberá mostrar las tendencias y conocimiento del personal de la Comisión Nacional de Seguros y Fianzas, al enfrentarse a situaciones comunes que involucran la seguridad.

OBJETIVO

Evaluar el nivel de concientización que el personal de la CNSF tiene hacia la seguridad de la información.

ALCANCE

Para este diagnóstico se seleccionará una muestra representativa de los empleados de la CNSF que hagan uso de activos de tecnológicos.

ACTIVIDADES

- Identificar audiencias.
- Aplicar encuestas.
- Recopilación de resultados
- Identificar el nivel de madurez del personal de la CNSF con respecto a la seguridad de la información haciendo uso de:
  - ✓ Sesiones de Trabajo.
  - ✓ Cuestionarios de selección de rubros de seguridad.
- Realizar informes de identificación del nivel de concientización.

ENTREGABLES

- Informe de nivel de concientización del personal de la CNSF.

PROYECTO VI. CLASIFICACIÓN Y PONDERACIÓN DE VULNERABILIDADES

OBJETIVOS

- Clasificar las vulnerabilidades en rubros específicos de seguridad basados en el estándar ISO/IEC 17799:2005
- Asignar una calificación cuantitativa a cada una de las vulnerabilidades identificadas dependiendo del impacto tecnológico que ocurra en la aplicación de negocio en caso que éstas sean explotadas

ALCANCE

- Todas las vulnerabilidades identificadas en la infraestructura tecnológica que soporta las aplicaciones críticas de negocio de la CNSF.

ACTIVIDADES

- Clasificación de las vulnerabilidades y deficiencias de control dentro de los rubros específicos de seguridad.
- Asignar valores cuantitativos a cada una de las vulnerabilidades clasificadas con base en el impacto tecnológico que pudiera ocurrir en caso que sean explotadas.

ENTREGABLES

- Clasificación y ponderación de vulnerabilidades y deficiencias de control en rubros específicos de seguridad. Los resultados son agrupados con base en el estándar ISO/IEC 17799:2005 referente a seguridad, obteniendo los siguientes **rubros** con sus respectivos niveles de **vulnerabilidad**.

  - ✓ A) Políticas de Seguridad
  - ✓ B) Seguridad Organizacional
  - ✓ C) Administración y Control de
  - ✓ Activos
  - ✓ D) Seguridad de Personal
  - ✓ E) Seguridad Física y Ambiental
  - ✓ F) Seguridad de Soporte y
  - ✓ Operaciones de Cómputo
  - ✓ G) Control de Acceso
  - ✓ H) Seguridad de Aplicaciones
  - ✓ I) Planeación de Recuperación
  - ✓ de Desastres
  - ✓ J) Cumplimiento

- Informe de clasificación y ponderación de vulnerabilidades.
- Matriz con las vulnerabilidades identificadas considerando al menos:
  - ✓ Herramienta utilizada.
  - ✓ Descripción de vulnerabilidad.
  - ✓ Referencia de acuerdo el ISO/IEC 17799:2005.
  - ✓ Forma de mitigación – alternativas de solución de la vulnerabilidad, considerando:
    - Solución administrativa.
    - Solución operativa.

- Solución técnica.

- Matriz con las deficiencias en controles identificadas considerando al menos:
  - ✓ Descripción del control.
  - ✓ Referencia de acuerdo el ISO/IEC 17799:2005.
  - ✓ Forma de mitigación – alternativas de solución de las deficiencias de control, considerando:
    - Solución administrativa.
    - Solución operativa.
    - Solución técnica.

- Lista de controles existentes y su madurez.

PROYECTO VII.- RECOMENDACIÓN PARA CORREGIR LAS VULNERABILIDADES

OBJETIVO

Se dará las recomendaciones para corregir las vulnerabilidades detectadas durante el programa de identificación para iniciar el análisis de riesgos bajo una plataforma actualizada.

ALCANCE

Vulnerabilidades identificadas y deficiencia de controles.

ACTIVIDADES

- Planeación de Correcciones.
  - ✓ Seleccionar el equipo de trabajo de corrección de vulnerabilidades.
  - ✓ Definir roles y responsabilidades.
  - ✓ Establecer los tiempos de ejecución.
- Realizar el análisis de impacto

ENTREGABLES

- Plan de trabajo.
- Organización del equipo, organigrama y asignación de roles y responsabilidades.
- Reporte de supervisión de análisis de impacto.

PROGRAMA III. ANÁLISIS DE RIESGOS

El análisis de riesgos será realizado considerando una Metodología de Administración de Riesgos y a través de su aplicación se deberá identificar de una manera asertiva y rápida la importancia relativa de los riesgos y el impacto que tendría en la Comisión Nacional de Seguros y Fianzas en caso de que alguno de estos riesgos se materializara, asimismo se deberán generar las estrategias de acción que deberá seguir para administrarlos de manera correcta.

OBJETIVO

Realizar el Análisis de Riesgos sobre los activos correspondientes a los procesos de la Dirección General de Informática, considerando las vulnerabilidades, amenazas e impactos al negocio, mediante el uso de metodologías de análisis de riesgos.

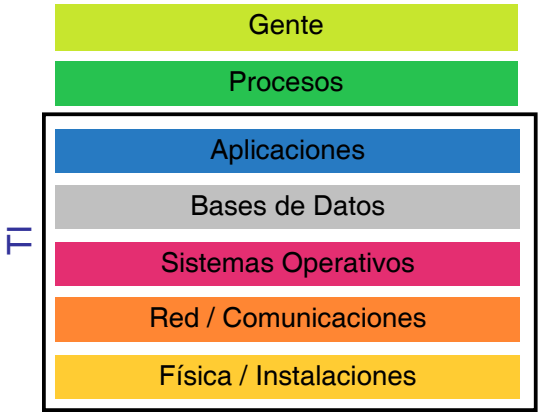
La Administración de Riesgos consistirá en decidir para cada uno de los riesgos identificados, si serán evitados, aceptados, transferidos o mitigados.

Adicionalmente se Identificarán los controles necesarios para lograr la mitigación de los riesgos.

ALCANCE

Identificar y clasificar todos los riesgos de la información asociados a los activos correspondientes a los procesos de la Dirección General de Informática, identificando las vulnerabilidades, amenazas, agentes e impactos en la Comisión Nacional de Seguros y Fianzas.

Lo anterior deberá realizarse conforme a la norma ISO/IEC 27001:2005 y la metodología de trabajo deberá considerar las siguientes capas:



ACTIVIDADES

Las actividades a realizar para el Análisis de Riesgos son:

- Evaluar sensibilidad de los activos
- Analizar vulnerabilidades
- Identificar las amenazas que podrían explotar las vulnerabilidades identificadas en los activos, así como su probabilidad de ocurrencia.
- Identificar el impacto que podría tener para la organización.
- Evaluar escenarios
- Revisar los controles ya existentes y el nivel de mitigación del riesgo.
- Identificar y priorizar los riesgos existentes.
- Es necesario hacer uso de metodologías de administración de riesgos.
- Para la determinación, priorización y evaluación de los riesgos, se deben considerar los factores cualitativos de la amenaza, vulnerabilidad, probabilidad e impacto que se obtuvieron.
- La determinación y priorización de riesgos debe realizarse mediante herramientas automatizadas para decisiones en grupo.
- Determinar las Estrategias de Administración de Riesgos considerando:

  - ✓ Incluir alternativas de aceptar, evitar, mitigar o transferir los riesgos identificados.
  - ✓ Se debe tener en cuenta la participación de personal de las diversas áreas de la institución (personal no técnico) para la determinación de los posibles impactos.
- Identificar y seleccionar los controles requeridos para mitigar aquellos riesgos que se hayan decidido.

ENTREGABLES

- Clasificación de los activos.
- Reporte de análisis de riesgos, alineado a los rubros definidos por el Estándar de Seguridad ISO/IEC 17799:2005.
  - ✓ Nivel de vulnerabilidad identificado para cada deficiencia de control y vulnerabilidad identificados.
  - ✓ Importancia relativa de cada riesgo identificado.
  - ✓ Mapa de riesgos que consideren los riesgos existentes clasificados por el impacto al negocio que ellos representan y con el nivel de vulnerabilidad existente en la infraestructura analizada.
- Lista de Acuerdos de Niveles de Servicio necesarios para los riesgos que se van a transferir.
- Lista de riesgos que serán aceptados.
- Lista de riesgos que serán evitados.
- Estrategia de Seguridad que permita a la Comisión Nacional de Seguros y Fianzas identificar el tratamiento que se le dará a los riesgos de seguridad identificados.
  - ✓ Estrategia propuesta para realizar los trabajos de implantación de seguridad informática considerando un análisis costo riesgos
  - ✓ Determinar las actividades y programas a realizar en un corto, mediano y largo plazo especificando tiempos y responsables para su realización.

- Definición el nivel máximo de riesgo aceptable
- Cálculo del Riesgo Residual. Con base a los controles que ya tenga en la organización y los que se van a implantar.

PROGRAMA V. DESARROLLO DE NORMATIVIDAD

El desarrollo de normatividad consiste en la creación de políticas, estándares y guías de seguridad para que se adecuen a las necesidades reales de la Comisión Nacional de Seguros y Fianzas, con el fin de proporcionar los lineamientos normativos de seguridad, que le permitan proteger sus activos.

V.1. DESARROLLO DE POLÍTICAS, ESTÁNDARES Y GUÍAS

OBJETIVO

Desarrollar las políticas, estándares y guías que ayuden a minimizar las vulnerabilidades identificadas en el Análisis de Riesgos.

ALCANCE

Las políticas, estándares y guías identificados para su desarrollo que consideren las vulnerabilidades identificadas en el Análisis de Riesgos.

ACTIVIDADES

Las actividades a realizar para la realización de las políticas, estándares y guías de seguridad son:

- Integrar los resultados del análisis de riesgos para el desarrollo de las políticas de seguridad.
- Analizar las políticas y normatividad que han sido desarrolladas actualmente.
- Desarrollar la política corporativa de seguridad de la Comisión Nacional de Seguros y Fianzas
- Desarrollar cada una de las políticas propuestas en el estándar internacional ISO/IEC 17799:2005, considerando los siguientes elementos:
  - ✓ Desarrollo de la política general de seguridad.
  - ✓ Desarrollo de estándares y guías necesarias y aplicables, que ayuden a minimizar las vulnerabilidades identificadas, además de sostener la política general de seguridad.
- Realizar actividades de aseguramiento de calidad que permitan garantizar que las vulnerabilidades identificadas sean corregidas con base a las políticas, estándares y guías desarrollados.

ENTREGABLES

- Normatividad: Políticas, estándares y guías de seguridad alineados al estándar internacional de seguridad ISO/IEC 17799:2005.

PROGRAMA VII. CONCIENTIZACIÓN (AWARENESS).

Se provee al personal interno de la Comisión Nacional de Seguros y Fianzas y externos relacionados, la conciencia de la seguridad de la información, sus razones y su importancia en la empresa y en la forma de operar.

VII.I.- PLAN DE CONCIENTIZACIÓN

OBJETIVO

Definir el plan de concientización a todo el personal de la CNSF.

ALCANCE

Todo el personal de la CNSF dependiendo de su rol y participación.

ACTIVIDADES

- Definir alcance, audiencias y contenido del programa de concientización.

ENTREGABLES

- Estrategia de concientización.
- Plan de concientización.

PROGRAMA VIII. CERTIFICACIÓN Y ACREDITACIÓN

El objetivo es certificar y acreditar las soluciones implementadas asegurando que dichas soluciones operarán a un nivel aceptable de riesgo y cumplan con las políticas y estándares de la organización.

VIII.I.- DEFINICIÓN

OBJETIVO

Definir y acordar la misión del proceso de certificación y acreditación de seguridad de las soluciones de seguridad implantadas.

ALCANCE

Todas las soluciones implantadas.

ACTIVIDADES

- Definir el alcance general del proceso de certificación y acreditación.
- Definir y desarrollar el documento del Sistema de Gestión de la Seguridad de la Información que contendrá, la organización, roles y responsabilidades de los participantes en el proceso.
- Desarrollar, afinar y aprobar el plan de trabajo.

ENTREGABLES

- Entrega de la documentación del Sistema de Gestión de la Seguridad de la Información, que debe comprender los requerimientos solicitados por el ISO/IEC 27001:2005, de los programas y proyectos solicitados, por mencionar aunque esto no es limitativo:
  - ✓ Implicación de la Dirección
  - ✓ Declaración del alcance del SGSI.
  - ✓ Política y objetivos de seguridad.
  - ✓ Inventario de todos los activos de información
  - ✓ Enfoque de evaluación de riesgos documentado (Descripción de la metodología de evaluación del riesgo)
  - ✓ Lista de amenazas, vulnerabilidades e impactos
  - ✓ Reporte de los impactos del negocio y las probabilidades
  - ✓ Plan de tratamiento de riesgos
  - ✓ Lista de objetivos de control y controles

- ✓ Registro de riesgos residuales aprobados
- ✓ Autorización de la administración para implementar el ISMS
- ✓ Declaración de aplicabilidad (statement of applicability)

PROGRAMA IX. CIERRE

El cierre se llevará a cabo una vez que se hayan finalizado todos los programas y proyectos señalados.

OBJETIVO

Se deberá presentar los resultados generales y formalizar el término del plan.

ALCANCE

Todos los resultados obtenidos en los programas anteriores.

ACTIVIDADES

- Realizar la presentación final de resultados.
- Realizar las cartas de término.
- Exponer la presentación de resultados finales.

ENTREGABLES

- Presentación final de resultados.
- CD con toda la información.
- Carta de terminación.

Actividades y entregables solicitados

Las actividades y entregables son los mencionados en los programas y proyectos descritos previamente.

Otras actividades que se deben realizar:

- Entrega semanal de los indicadores correspondientes al Análisis del Valor Ganado
- Elaboración de todos los documentos para la coordinación del plan, tales como calendario, minutas de trabajo, etc.
- Descripción del equipo de trabajo y calendario de actividades.
- En todos los actividades y entregables (los que procedan) se deberán alinear con base en el ISO 27001, el cual no es de carácter limitativo y se puede enriquecer con algún estándar adicional:
  - ✓ COBIT (Control Objectives for Information and Related Technology).
  - ✓ EDP Auditing.
  - ✓ Auerbach Knowledge Base.
  - ✓ Best Practices de controles de aplicación.
  - ✓ Information System Audit and Control Association (ISACA).
  - ✓ White Papers de Seguridad Física, Auditoria a centros de cómputo y Seguridad en centros de cómputo.

- ✓ Core de Políticas de Seguridad.
- ✓ NIST (National Institute of Standards and Technology).

Capítulo 4. Planeación de los recursos

En este capítulo se determinarán la cantidad de recursos necesarios para ejecutar las actividades que se han establecido en los programas y proyectos referidos para la implantación del Sistema de Gestión de la Seguridad de la Información en la Comisión Nacional de Seguros y Fianzas.

4.1. Contratación de servicios necesarios

Es importante mencionar, que la implantación de un Sistema de Gestión de la Seguridad de la Información es una actividad que requiere demasiada especialización, por lo que se contratará un servicio de terceros que brinde este apoyo, independientemente de los empleados de la CNSF que participarán en su implantación.

Para la empresa que dará la consultoría y los recursos que proveerá, se solicitarán requisitos mínimos para garantizar su experiencia.

Con respecto a la empresa se solicitará que tenga al menos 3 años de antigüedad en el mercado, desempeñando el giro o actividad relacionada con la implantación de sistemas de gestión de la seguridad de la información.

Mientras que los recursos humanos que proporcione el proveedor, deberán cumplir con los perfiles, experiencia, certificaciones y cantidad de recursos que se menciona en la tabla 4.1.

Suministrador	Nombre del Rol	Descripción del Rol	Cantidad de Recursos	Perfil solicitado
CNSF	Coordinador de las áreas usuarias de la CNSF	Coordinar las tareas de las áreas usuarias involucradas en el desarrollo del proyecto.	1	
CNSF	Usuarios Involucrados	Participar en las actividades definidas en los planes de trabajo, que se establezcan en conjunto con personal de la CNSF y el equipo de trabajo del proveedor. Entre algunas de sus actividades se consideran: • Apoyar al desarrollo del proyecto. • Validar los productos (en la medida de su competencia).	Las Direcciones Generales de la CNSF	
Proveedor	Administrador de Proyecto (AP)	Responsable final del resultado del proyecto. Encargado de llevar a cabo todos los procesos de administración del proyecto y su documentación. Algunas de sus funciones más importantes y que figuran como factores de éxito son: verificación de que los productos se terminen a tiempo y con la calidad que el usuario haya especificado, revisión del avance del proyecto contra lo establecido en el plan de trabajo, celebración de las reuniones de trabajo y presentación del avance.	1	✓ Deberá tener como mínimo 3 años de experiencia comprobables en haber participado en proyectos como administrador de proyecto en la realización de alguna de las fases o etapas en la implantación de proyectos de Seguridad Informática. ✓ Deberá estar presente hasta la terminación del proyecto. ✓ Este rol no puede desempeñar QA, EH y ES.
Proveedor	Quality Assurance (QA)	Responsable de asegurar que los entregables tengan la presentación y el contenido solicitado para la implantación de un SGSI y que éste se pueda certificar en ISO 27001.	1	✓ Deberá tener como mínimo 5 años de experiencia comprobables en áreas de Seguridad y Auditoría Informática. ✓ Contar con al menos dos de las siguientes certificaciones: CISA, CISSP, CISM ó ISO27001Auditor Líder ✓ Este rol no puede desempeñar otro rol distinto a lo largo del proyecto.

Proveedor	Ethical Hackers (EH)	Realiza pruebas de penetración y el análisis de vulnerabilidades.	1	✓ Deberá tener como mínimo 2 años de experiencia comprobables en áreas de Seguridad y Auditoría Informática. ✓ Deberá demostrar que ha desempeñado actividades de pruebas de penetración y análisis de vulnerabilidades por lo menos con tres clientes. ✓ Tener al menos una de las siguientes certificaciones: CISA, CISSP, CISM, ISO27001 ó alguna certificación reconocida internacionalmente de hackeo ético. ✓ Este rol no puede desempeñar AP, QA e IM.
Proveedor	Implantadores de SGSI (IM)	Encargado de conducir y documentar la implantación del SGSI y los requisitos que solicita el ISO 27001.	2	✓ Deberá tener como mínimo 3 años de experiencia comprobables en áreas de Seguridad y Auditoría Informática ✓ Tener al menos una de las siguientes certificaciones: CISA, CISSP, CISM ó ISO27001. ✓ Este rol no puede desempeñar QA, y ES.
Proveedor	Especialistas (ES)	Ejecutan las actividades identificadas en el Plan de Actividades	4	✓ Deberá tener como mínimo 1 año de experiencia comprobables en áreas de Seguridad, Riesgos, Continuidad del Negocio y Auditoría Informática ✓ Este rol no puede desempeñar AP, QA e IM.

Tabla 4.1. Perfil de los recursos humanos

Ahora los requerimientos materiales que se necesitarán por parte del proveedor, son los que se muestran en la tabla 4.2.

Suministrador	Nombre del Producto	Características	Cantidad
Proveedor	Estaciones de Trabajo	El proveedor deberá suministrar las computadoras necesarias para las personas que asigne al proyecto.	Los necesarios
Proveedor	Software para realizar el análisis de riesgo, detectar vulnerabilidades y todas las actividades solicitadas *	El proveedor deberá traer el software necesario para hacer el trabajo solicitado, sin costo adicional a la CNSF.	El necesario

Tabla 4.2. Características de los requerimientos materiales

***** Características que debe tener el software:

- Deberá tener la facilidad de realizar actualización en línea desde Internet, lo que permite contar con las últimas vulnerabilidades identificadas por el proveedor de la herramienta.

- No deberán representar ningún riesgo para la seguridad de los equipos e información de la CNSF.

- En caso de no tener software para el análisis de vulnerabilidades el proveedor deberá tener una Base de datos de vulnerabilidades y alternativas de solución.

4.2. Recursos materiales

Los recursos materiales necesarios para la implantación del Sistema de Gestión de la Seguridad de la Información, se deberán considerar para los empleados de la CNSF y para las personas que traerá el proveedor.

Para los empleados de la CNSF, no se requiere material adicional con el que cuentan en este momento, pero para las personas que traiga el proveedor, se deberá considerar los recursos materiales que se especifican en la tabla 4.3.

Suministrador	Nombre del Producto	Características	Cantidad
CNSF	Lugares de Trabajo	Con sillas, 1 línea telefónica (para efectos de localización), conexiones y usuarios de red y a la base de datos; acceso a servicios de impresión e Internet.	Los necesarios
CNSF	Documentación	Técnica y de usuario de la aplicación	La necesaria

Tabla 4.3. Recursos materiales

4.3. Recursos económicos

Los recursos económicos adicionales que se requieren para la implantación del Sistema de Gestión de la Seguridad de la Información, son los que se especifican en la tabla 4.4.

Tipo de Recurso	Cantidad		Nota
Personal CNSF	-	-	*No se requiere ampliar la nómina*
Servicios de Consultoría		*1,820,000.00*	
Consultoría para la implantación de un SGSI	1,800,000.00		
Certificación ISO 27001	20,000.00		
Materiales		*5,000,000.00*	
Equipo de Cómputo	-		Ya se tiene
Sillas y Escritorios	-		Ya se tiene
Teléfono	-		Ya se tiene
Acceso de red de la CNSF	-		Ya se tiene
Adquisición de hardware y software de seguridad	5,000,000.00		Se determina con mayor precisión después de la consultoría
Total		**6,820,000.00**	

Tabla 4.4. Recursos económicos

Capítulo 5. Implantación y Control

En este capítulo se llevarán a acabo las decisiones hechas en las fases anteriores, controlando su implantación y subsiguiente desarrollo.

5.1. Implantación

En esta etapa se debe decidir quién será responsable de hacer qué y cuándo, de tal manera que para la implantación del Sistema de Gestión de la Seguridad de la Información en la Comisión Nacional de Seguros y Fianzas, se propone el siguiente plan que contiene la información siguiente:

- Las actividades a desarrollar
- Los recursos humanos que se encargarán de atender las actividades
- Los días que durará cada actividad
- Las fechas en que se ocuparán los recursos humanos
- Los entregables que se producirán al realizar la actividad.

En la figura 5.1. se muestra la información que tiene el plan de actividades.

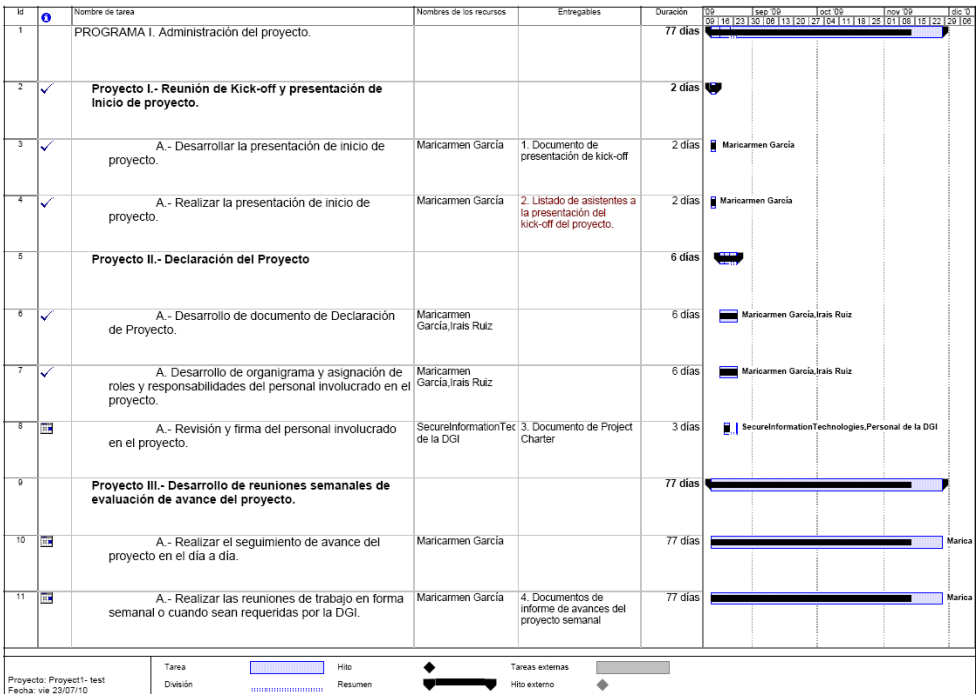


Figura 5.1. Plan de actividades

En la sección de Anexos viene el plan con todas las actividades para su consulta.

5.2. Control de los planes y la planeación

En esta etapa se realizará la identificación de variables, la definición de los criterios de medición y se diseñaran los indicadores, que generen un sistema de información que permitan evaluar y adoptar las acciones correspondientes cuando se presenten desviaciones a los planes y a la planeación.

Este sistema de información estará integrado por los siguientes indicadores que permitirán evaluar el ideal y los objetivos establecidos en el punto **2.5 Determinación de los Fines de la Planeación,** con el propósito que al momento de presentarse desviaciones se adopten las acciones correctivas correspondientes.

Ideal

- Diseñar e implantar una solución integral de seguridad de la información, para lograr el aseguramiento de sus procesos de negocio e incrementar la confiabilidad en su operación

Indicadores y Criterios de Medición

- El número de veces que se requirió utilizar los mecanismos de seguridad y no fue posible seguir operando *debe ser ninguna o cero veces al año*

Objetivos de TI

- Asegurar que los servicios de TI están disponibles según se requieran.
- Asegurar un mínimo impacto al negocio en caso de una interrupción o cambio en los servicios de TI.
- Asegurar que los servicios y la infraestructura de TI pueden resistir y recuperarse de fallas originadas por un error, ataque deliberado o desastre.
- Garantizar que la información crítica y confidencial esté prohibida a aquellos que no tienen acceso a ella.
- Garantizar que las transacciones e intercambios de información automatizados del negocio sean confiables.
- Mantener la integridad de la información y de la infraestructura de procesamiento.
- Proteger y mantener registro de todos los activos de TI.

Indicadores y Criterios de Medición

- El número de horas perdidas por usuario por año debido a interrupciones no planeadas *sea menor al equivalente de 4 días contando fines de semana*
- El número de incidentes con impacto al negocio sea ninguno.
- El número de sistemas que no cumplen con los requerimientos de seguridad sea menor al 10% con respecto a todos los sistemas.

- El tiempo para otorgar, cambiar o eliminar privilegios de acceso sea menor a 8 horas hábiles.

Metas de Proceso

- Establecer un plan de continuidad de TI que soporte los planes de continuidad del negocio.
- Desarrollar planes de continuidad de TI que puedan ejecutarse, probarse y mantenerse.
- Minimizar la posibilidad de interrupción de los servicios de TI.
- Permitir el acceso a información crítica y sensible sólo a usuarios autorizados.
- Identificar, monitorear y reportar vulnerabilidades e incidentes de seguridad.
- Detectar y resolver accesos no autorizados a la información, aplicaciones e infraestructura.
- Minimizar el impacto de las vulnerabilidades y de los incidentes de seguridad.

Indicadores y Criterios de Medición

- El porcentaje de acuerdos de niveles de servicios (SLAs) de disponibilidad que se cumplen debe *ser mayor al 95%*
- El número de procesos críticos del negocio que dependen de TI, no cubiertos por un plan de continuidad *debe ser ninguno o cero*
- El porcentaje de pruebas para lograr los objetivos de recuperación *debe ser menor al 10%*
- La frecuencia en la interrupción de servicios de sistemas críticos *no debe exceder de ocho horas al mes*
- El número y tipo de violaciones de acceso reales y sospechosas *sean cero.*
- El número de violaciones en la segregación de funciones *sean cero*
- El porcentaje de usuarios que no cumplen con los estándares de contraseñas sea cero.
- El número y tipo de código malicioso prevenido sea mayor al 95%

Metas de Actividades

- Desarrollar y mantener (mejorar) los planes de contingencia de TI
- Capacitación y pruebas de los planes de contingencia
- Almacenamiento de copias de los planes de contingencia fuera de las instalaciones
- Entendimiento de los requerimientos, vulnerabilidades y amenazas de seguridad.
- Administración de las identidades y autorizaciones de los usuarios de manera estándar.
- Definición de incidentes de seguridad.
- Pruebas de seguridad regulares.

Indicadores y Criterios de Medición

- El tiempo transcurrido entre las pruebas de cualquier elemento dado del plan de continuidad de TI *no debe exceder de un mes*
- El número de horas de capacitación por año de cada empleado relevante de TI *debe ser al menos de 40 horas*
- Porcentaje de componentes de infraestructura críticos con monitoreo de disponibilidad automatizado *debe ser del 100%*
- Frecuencia de revisión del plan de continuidad de TI *debe ser por lo menos una vez al año*
- La frecuencia y revisión del tipo de eventos de seguridad a ser monitoreados *sea al menos una vez al día.*
- El número y tipo de cuentas obsoletas *sea cero*
- El número de direcciones IP no autorizadas, puertos y tipos de tráfico denegados *sea cero*
- El porcentaje de llaves criptográficas comprometidas y revocadas *sea menor al 5% de todas*
- El número de derechos de acceso autorizados, revocados, restaurados o cambiados sea cero.

Conclusiones

El principal objetivo de este trabajo fue presentar cómo implantar un Sistema de Gestión de la Seguridad de la Información “SGSI” en la Comisión Nacional de Seguros y Fianzas “CNSF”, lo cual se logró mediante el proceso de conducción (proceso de cambio controlado del objeto conducido, que en este caso es la Dirección General de Informática), que considera a la planeación como una actividad fundamental que apoya a este proceso.

Esta actividad de planeación se basó en el enfoque idealizado que resultó ser una excelente guía para realizar las diferentes actividades que permitieron la visualización y especificación de la Dirección General de Informática “DGI”, el establecimiento de los objetivos de conducción y las actividades que permiten realizar este cambio de manera directa, a través de programas y proyectos, que contribuyan al cambio del estado actual al estado deseado.

También se logró con el enfoque del diseño idealizado simplificar este proceso de planeación, ya que desde un principio se establece un estado desde donde uno quiere estar, reduciendo el número de alternativas que deben considerarse al decidir cómo se va a llegar hasta allí, además de que en muchos casos los obstáculos desaparecen.

Adicionalmente, con el diseño idealizado se logró que la pertenencia del plan resultante esté muy repartida entre los que deben implantarlo, evitando la resistencia. Adicionalmente, quienes participaron en su preparación llevaron a cabo con entusiasmo la implantación de su diseño y de un plan basado en él, ya que la planeación fue participativa.

Por otra parte, para determinar la problemática de la CNSF, se utilizaron las herramientas de análisis de las causas raíz del problema tales como los diagramas de Causa-Efecto (Ishikawa) así como Gráficas de Pareto, con lo cual se logró identificar que los usuarios no contaban con la información de manera confidencial, oportuna e integra para desempeñar sus labores de supervisión, siendo esto el problema real que se solucionó con la implantación del SGSI en la CNSF

Con las ideas de Checkland, se consiguió entender el impacto de la implantación de un SGSI en la CNSF, ya que se identificaron a los actores y beneficiados involucrados en el sistema, también se logró conceptualizar el problema al que nos enfrentamos en donde un sistema se debe de ver como un sistema total, esto es, considerar el sistema del que forma parte (suprasistema) y sus relaciones, así como los elementos del sistema (subsistemas) en función del sistema y suprasistema que los contienen.

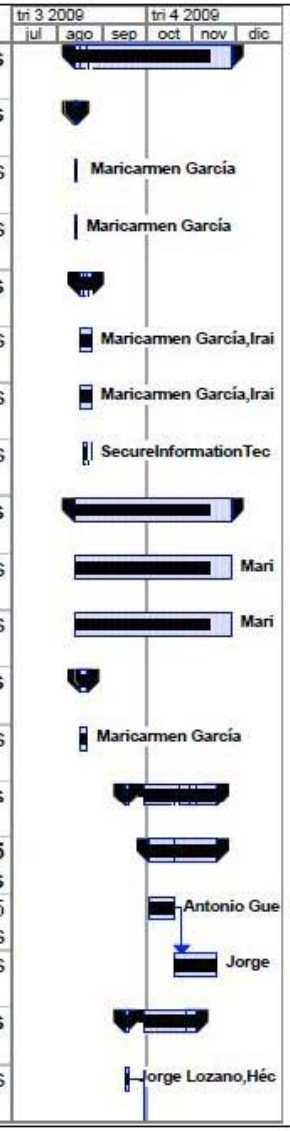
Como último punto, una organización mejora su nivel de seguridad cuando empieza a implantar soluciones más administrativas, como el uso de políticas y procedimientos, que complementan las soluciones técnicas con las que ya contaba. Madurar un sistema de gestión de la seguridad de la información, en última instancia es un cambio cultural y, como todo camino hacia la madurez, requiere de tiempo, esfuerzo y paciencia, pero una vez que se adopta y se hace de una disciplina, los resultados se podrán percibir desde el momento en que se empieza a aplicar lo que se sabe y a hacer lo que se quiere.

Bibliografía

1.- Ackoff, Russell. Planificación de la empresa del futuro. Limusa,1983.
2.- COBIT® 4.1 (2005)
3.- ISO 27001® (2008)
4.- ITIL® 1.1 (2001)
5.- Willian W.Hines, Douglas C.Montgomery .Probabilidad y estadística para Ingeniería
6.- Gelman O. & Negroe G. La planeación como un proceso básico en la conducción. Revista de la Academia Nacional de Ingeniería, 1982, Vol. I No. 4, México.
7.- Ramírez Rafael, Selsky John W., Van der Hejden, Kees. Business Planning for Turbulent Times. New Methods for Applying Scenarios. Earthscan, 2008
8.- Gabriel Sánchez Guerrero. Técnicas Participativas de Planeación. Fundación ICA, A.C.,2003.
9.- Checkland, P. Pensamiento de Sistemas, Práctica de Sistemas. Wiley,1993.
10.- Beer S. What is Cybernetics? Kibernetes, Emerald Editors, Vol. 31, Issue 2, 2002.
11.- Gelman O. Desastres y Protección Civil: Fundamentos de Investigación Interdisciplinaria. Universidad Nacional Autónoma de México, Dirección General de Asuntos de Personal Académico, Instituto de Ingeniería, 1996.
12.- Comisión Nacional de Seguros y Fianzas. INVITACION DE CARÁCTER NACIONAL A CUANDO MENOS TRES PERSONAS INV/008/07. (2007)
13.- Comisión Nacional de Seguros y Fianzas. Solicitudes DGI-H. (2008)
14.- Alan P. Brache y Sam Bodle-Scott. Implementación. McGrawHill, 2006
15.- Project Management Institute Publications, A Guide to the Project Management Body of Knowlegde: Fourth Edition. PMI, 2009.

ANEXOS

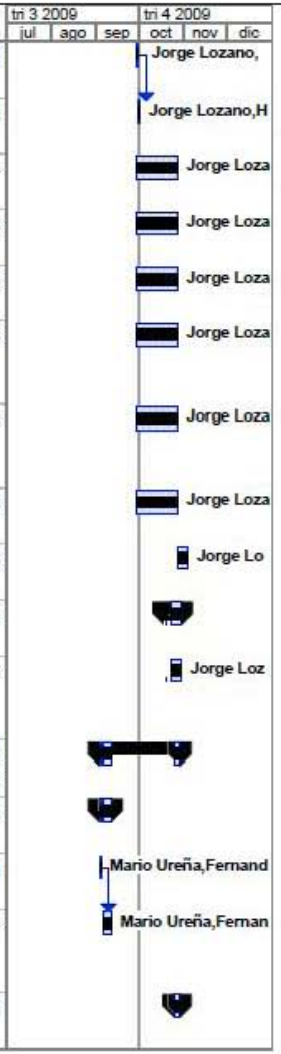
Id		Nombre de tarea	Nombres de los recursos	Entregables	Duración
1		PROGRAMA I. Administración del proyecto.			**77 días**
2	✓	**Proyecto I.- Reunión de Kick-off y presentación de Inicio de proyecto.**			**2 días**
3	✓	A.- Desarrollar la presentación de inicio de proyecto.	Maricarmen García	1. Documento de presentación de	2 días
4	✓	A.- Realizar la presentación de inicio de proyecto.	Maricarmen García	2. Listado de asistentes a la	2 días
5		**Proyecto II.- Declaración del Proyecto**			**6 días**
6	✓	A.- Desarrollo de documento de Declaración de Proyecto.	Maricarmen García,Irais Ruiz		6 días
7	✓	A. Desarrollo de organigrama y asignación de roles y responsabilidades del personal involucrado en	Maricarmen García,Irais Ruiz		6 días
8		A.- Revisión y firma del personal involucrado en el proyecto.	SecureInformation de la DGI	3. Documento de Project Charter	3 días
9		**Proyecto III.- Desarrollo de reuniones semanales de evaluación de avance del proyecto.**			**77 días**
10		A.- Realizar el seguimiento de avance del proyecto en el día a día.	Maricarmen García		77 días
11		A.- Realizar las reuniones de trabajo en forma semanal o cuando sean requeridas por la DGI.	Maricarmen García	4. Documentos de informe de avances	77 días
12	✓	**Proyecto IV.- Plan detallado de actividades del proyecto**			**5 días**
13	✓	A.- Desarrollar un plan de actividades del proyecto.	Maricarmen García	5. Documento de plan de actividades	5 días
14	✓	PROGRAMA II. Análisis de vulnerabilidades y pruebas de penetración.	**Héctor Gutiérrez,Jorge**		**44 días**
15	✓	**Proyecto I.- Desarrollo de Análisis de brecha de ISO/IEC 27001:2005**			**32.25 días**
16	✓	A.- Desarrollar el análisis de brecha conforme a la norma ISO/IEC 27001:2005 en la DGI de la CNSF.	Antonio Guevara,Jorge	6. Documento de Análisis de brecha	11.25 días
17	✓	A.- Verificar los controles de seguridad existentes y realizar un inventario de los mismos.	Jorge Lozano	7. Listado de controles existentes	21 días
18	✓	**Proyecto II.- Análisis de Vulnerabilidades y pruebas de penetración en la infraestructura de la CNSF.**			**34 días**
19	✓	A.- Definir con el personal de la DGI relacionado con el proyecto los objetivos a revisar.	Jorge Lozano,Héctor		2 días



Proyecto: Proyect1- test
Fecha: jue 22/07/10

Tarea — Hito — Tareas externas
División — Resumen — Hito externo
Progreso — Resumen del proyecto — Fecha límite

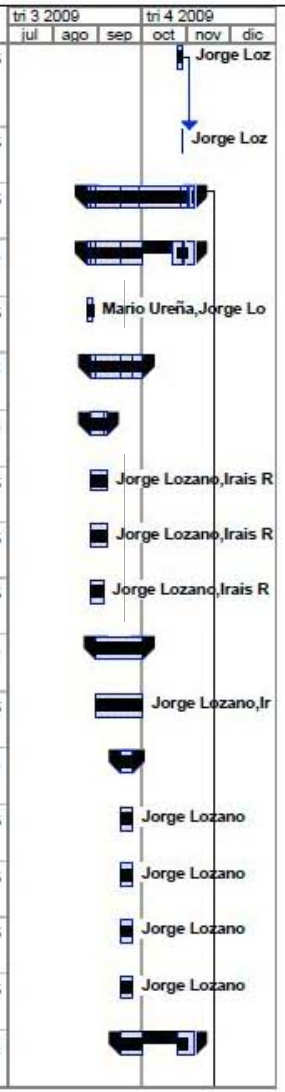
Id		Nombre de tarea	Nombres de los recursos	Entregables	Duración
20	✓	A.- Definir tiempos para las pruebas.	Jorge Lozano,Héctor		1 día
21	✓	A.- Afinar el alcance de las pruebas con el personal de la CNSF.	Jorge Lozano,Héctor		1 día
22	✓	A.- Realizar Análisis de Vulnerabilidades y pruebas de Hackeo Ético sobre la red de la CNSF.	Jorge Lozano,Héctor		20 días
23	✓	A.- Realizar la identificación y el análisis de las vulnerabilidades existentes en la infraestructura de red	Jorge Lozano,Héctor		20 días
24	✓	A.- Realizar análisis de vulnerabilidades, pruebas de penetración y hackeo ético sobre la red	Jorge Lozano,Héctor		20 días
25	✓	A.- Realizar análisis de vulnerabilidades sobre todos los segmentos de red de la CNSF y los servicios de hosting que se tengan con los proveedores, así	Jorge Lozano,Héctor Gutiérrez,Antonio		20 días
26	✓	A.- Las herramientas de identificación de vulnerabilidades y hackeo ético se configurarán en su nivel de revisión más estricto, con la finalidad de	Jorge Lozano,Héctor Gutiérrez,Antonio	9. Documento técnico con los pasos que se siguieron en	20 días
27	✓	A.- Realizar actividades relacionadas en compañía del personal designado de la CNSF	Jorge Lozano,Héctor		20 días
28	✓	A.- Desarrollar un documento de metodología, hallazgos, recomendaciones y pasos que se siguieron	Jorge Lozano,Héctor	8. Documentación con todos los	5 días
29	✓	**Proyecto III.- Recomendación para corregir las Vulnerabilidades detectadas**			**9.5 días**
30	✓	A.- Desarrollar un documento donde por cada vulnerabilidad detectada se recomiende la solución o corrección de acuerdo a las mejores prácticas que le	Jorge Lozano	10. Documento de recomendaciones de solución para cada	5 días
31		PROGRAMA III. PROGRAMAs del SGSI: Planificar			**39.75 días**
32	✓	**Proyecto I.- Revisión de la Política de Seguridad de la Información**			**6 días**
33	✓	A.- Revisar y dar las recomendaciones sobre la política de seguridad de la información de la DGI de	Mario Ureña,Fernando	12. Documento con las recomendaciones	1 día
34	✓	A.- Asegurar que la política cumpla con un ciclo de mejora continua y contemplar el procedimiento de formalización de la política de seguridad.	Mario Ureña,Fernando Olvera,Raúl		5 días
35		**Proyecto II.- Definición del alcance y límites del SGSI**			**3.75 días**



Proyecto: Proyect1- test
Fecha: jue 22/07/10

Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite

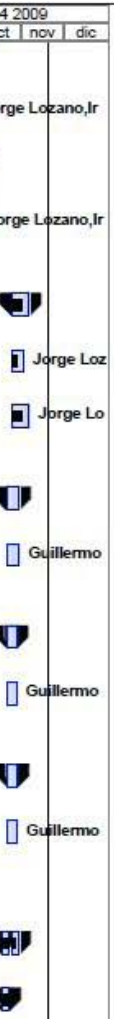
Id		Nombre de tarea	Nombres de los recursos	Entregables	Duración
36	✓	A.- Desarrollar el documento de alcance para el SGSI de la Dirección de Informática de la CNSF que contemple los objetivos y los límites del SGSI,	Jorge Lozano	13. Documento de definición del alcance y limites del SGSI de	3 días
37		A.- Revisar este documento con el personal de CNSF para su validación.	Jorge Lozano,Raúl		0.75 días
38		PROGRAMA IV. PROGRAMAs del SGSI: Hacer			54 días
39		**Proyecto I. Gestión de Riesgos**			**54 días**
40	✓	a. Enfoque de evaluación de riesgos de la DGI	Mario Ureña,Jorge		4 días
41	✓	**b. Identificar los riesgos**			**26 días**
42	✓	**i. Actualización de Diagramas de Riesgos de Proceso**			**7.33 días**
43	✓	A - Realizar entrevistas y validar diagramas de riesgos de proceso por los líderes de las áreas	Jorge Lozano,Irais	14b. Listado de entrevistas de	7 días
44	✓	A.- Actualizar los diagramas de riesgos de proceso de la DGI	Jorge Lozano,Irais		7 días
45	✓	A.- Generar los nuevos diagramas de riesgos de proceso que en su caso apliquen	Jorge Lozano,Irais	14. Diagramas de Riesgos de Proceso	7 días
46	✓	**ii. Actualización de activos**			**24 días**
47	✓	A.- Desarrollar un inventario de los activos más importantes de la DGI de la CNSF organizados	Jorge Lozano,Irais	15. Listado actualizado de los	24 días
48	✓	**iii. Actualización de Vulnerabilidades, Amenazas e Impactos**			**6 días**
49	✓	A.- Revisar las amenazas a que están expuestas los activos.	Jorge Lozano		6 días
50	✓	A.- Revisar las vulnerabilidades bajo las cuales podrían actuar las amenazas.	Jorge Lozano		6 días
51	✓	A.- Identificar los impactos que sobre los activos puede tener una perdida de confidencialidad,	Jorge Lozano		6 días
52	✓	A.- Actualizar con respecto a la situación actual estas vulnerabilidades, amenazas e impactos.	Jorge Lozano	16. Listado de vulnerabilidades,	6 días
53		**c. Estimar los riesgos**			**37 días**



Proyecto: Proyect1- test
Fecha: jue 22/07/10

Tarea — Hito — Tareas externas
División — Resumen — Hito externo
Progreso — Resumen del proyecto — Fecha límite

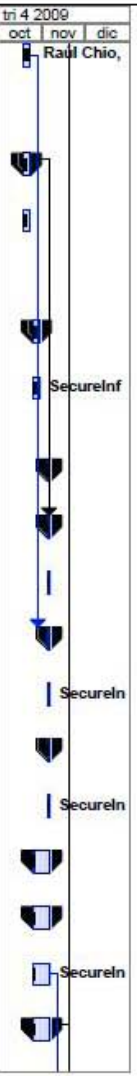
Id	Nombre de tarea	Nombres de los recursos	Entregables	Duración
54	**i. Estimar los niveles de impacto**			**6.5 días**
55	A.- Identificar impactos sobre los efectos en la actividad de la DGI.	Jorge Lozano,Irais	17. Documento de evaluación de	5 días
56	**ii. Revisión y actualización de Probabilidad**			**11 días**
57	A.- Revisar y actualizar la probabilidad de ocurrencia de fallas de seguridad derivada de las amenazas, vulnerabilidades e impactos	Jorge Lozano,Irais Ruiz,Fernando	18. Listado de probabilidades de ocurrencia revisadas	11 días
58	**iii. Revisar y actualizar los niveles de riesgo y las opciones de tratamiento de riesgo**			**10 días**
59	A.- Revisar y actualizar los niveles de riesgo y opciones de tratamiento de riesgo existentes en	Jorge Lozano,Raul	19. Listado de niveles de riesgo y	6 días
60	A.- Identificar y evaluar los niveles de riesgo y opciones de tratamiento de riesgo existentes en la infraestructura actual de la DGI para los	Jorge Lozano,Comité de	21. Reporte Ejecutivo del resultado del análisis de riesgos	10 días
61	**d. Seleccionar los objetivos de control y los controles para el tratamiento de riesgos**			**7 días**
62	A.- Realizar la selección de controles del Anexo A de la norma ISO/IEC 27001:2005 de acuerdo a los requerimientos identificados en el análisis y	Guillermo Orozco,Raul Chio,Antonio	22. Documento con la selección de controles del Anexo	7 días
63	**e. Plan de Tratamiento de Riesgos**			**4 días**
64	A.- Desarrollar el plan de tratamiento de riesgos donde se detallen las acciones a realizar, responsables, recursos necesarios y las prioridades	Guillermo Orozco,Raul Chio,Antonio	23. Documento plan de tratamiento de riesgos donde se	4 días
65	**f. Desarrollo de Declaración de Aplicabilidad**			**4.8 días**
66	A.- Desarrollar la declaración de aplicabilidad de acuerdo al análisis de riesgos y el análisis de brecha realizado, indicando los objetivos de control y controles seleccionados, existentes y las	Guillermo Orozco,Raul Chio,Antonio Guevara,Jorge	24. Documento de Declaración de Aplicabilidad avalada por la DGI.	4.8 días
67	**Proyecto II.- Manual del SGSI**			**10 días**
68	**a. Revisión de Manual del SGSI**			**5 días**



Proyecto: Proyect1- test
Fecha: jue 22/07/10

Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite

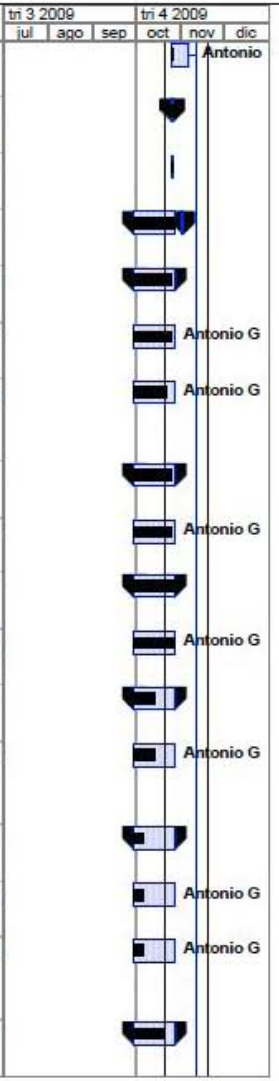
Id	Nombre de tarea	Nombres de los recursos	Entregables	Duración
69	A.- Revisar, dar recomendaciones de solución de hallazgos detectados, realizar las adecuaciones pertinentes, validar el documento y realizar la liberación del Manual del SGSI de la DGI.	Raúl Chio,Fernando Olvera,Beatriz Sánchez,Maricarm	25. Listado de observaciones y correcciones en el Manual del SGSI de	5 días
70	**b. Revisión del Procedimiento de Definición de la Documentación**			**5 días**
71	A.- Revisar, dar recomendaciones de solución de hallazgos detectados, realizar las adecuaciones pertinentes, validar el documento y realizar la liberación del Procedimiento de Definición de la		27. Listado de observaciones y correcciones del Procedimiento de	5 días
72	**c. Revisión de Procedimiento de Control de Documentos y Registros relacionados con el SGSI**			**5 días**
73	A.- Revisar, dar recomendaciones de solución de hallazgos detectados, realizar las adecuaciones pertinentes, validar el documento y realizar la	SecureInformation	29.Listado de observaciones y correcciones del	5 días
74	**Proyecto III.- Implementar Controles**			**2 días**
75	**a. Desarrollo de Objetivos de Control y Controles**			**2 días**
76	A.- Revisar y corregir los documentos de objetivos de control y controles.		31. Listado de observaciones y	2 días
77	**b. Desarrollo de Indicadores de Desempeño**			**2 días**
78	A.- Desarrollar indicadores de desempeño para los indicadores del SGSI de la DGI.	SecureInformation	33. Documento de Indicadores de	2 días
79	**Proyecto IV.- Revisión de Políticas de Seguridad de la Información**			**2 días**
80	A.- Revisar y corregir las políticas de seguridad de la información conforme sea necesario para dar soporte a	SecureInformation	34. Documentos de Políticas de	2 días
81	**Proyecto V.- Revisión de Procesos y Procedimientos de Seguridad de la Información**	**SecureInformatio**		**10 días**
82	**a. Desarrollo de los procedimientos de los objetivos de control A.13 del Anexo A del ISO/IEC**			**10 días**
83	A.- Desarrollar los procedimientos para cumplir con los objetivos de control A.13.1 y A.13.2.	SecureInformation	35. Procedimientos para cumplir con los	10 días
84	**b. Revisión de Procedimientos de Seguridad de la Información**			**10 días**



Proyecto: Proyect1- test
Fecha: jue 22/07/10

Tarea — Hito — Tareas externas
División — Resumen — Hito externo
Progreso — Resumen del proyecto — Fecha límite

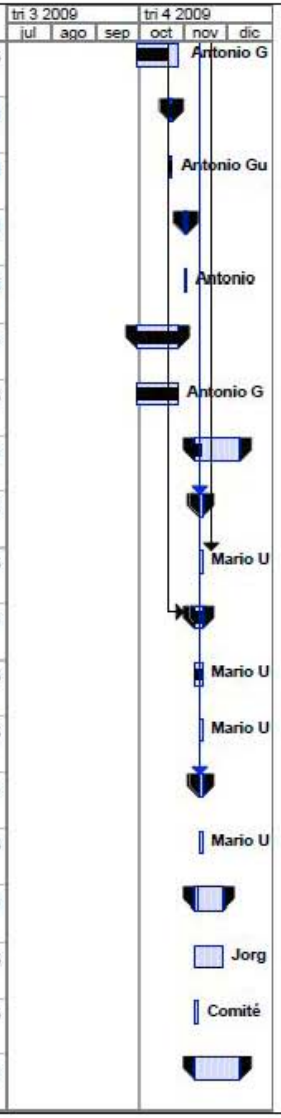
Id	Nombre de tarea	Nombres de los recursos	Entregables	Duración
85	A.- Revisar y actualizar los procedimientos de seguridad de la información para proveer soporte a	Antonio Guevara,Jorge	36. Documentos de Procedimientos de	10 días
86	**c. Desarrollo de Formatos de Documentación de Registros**			**1 día**
87	A.- Revisar y actualizar los formatos de documentación de registros basados en los		37. Formatos de Documentación de	1 día
88	**Proyecto VI.- Definición de estrategias de continuidad**	**Antonio Guevara,Jorge**		**24 días**
89	**a. Revisión de actividades necesarias para la operación**			**20 días**
90	A.- Realizar un análisis de las actividadesde la DGI de la CNSF evaluadas desde el punto de vista de su	Antonio Guevara,Jorge	38. Listado de actividades en orden	20 días
91	A.- Una vez que se tengan los resultados, realizar una sesión donde se discuta el orden de las actividades y desde el punto de vista del personal	Antonio Guevara,Jorge Lozano,Irais		20 días
92	**b. Determinar dependencias**			**20 días**
93	A.- Analizar por cada actividad que haya resultado como importante, cuáles son aquellas actividades	Antonio Guevara,Jorge	39. Listado de actividades con sus	20 días
94	**c. Obtención de métricas por actividad**			**20 días**
95	A.- Por cada una de las actividades que hayan resultado de importancia se obtendrán las métricas	Antonio Guevara,Jorge	40. Documento con las Métricas	20 días
96	**d. Determinar recursos necesarios para cada actividad**			**20 días**
97	A.- Analizar por cada actividad que haya resultado como importante, cuáles son sus requerimientos para un adecuado funcionamiento y que elementos	Antonio Guevara,Jorge Lozano,Irais	41. Documento con el Listado de actividades con sus	20 días
98	**e. Revisión de cumplimientos y requerimientos legales, regulatorios y contractuales**			**20 días**
99	A.- Generar una lista de las leyes, regulaciones, contratos y otros documentos que la CNSF requiera	Antonio Guevara,Jorge	42. Documento donde se enumeren	20 días
100	A.- Evaluar de entre la lista generada aquellos que impliquen penalizaciones por incumplimiento o por no prestar el servicio y generar un documento donde	Antonio Guevara,Jorge Lozano,Irais		20 días
101	**f. Desarrollo de matriz de impacto**			**20 días**



Proyecto: Proyect1- test
Fecha: jue 22/07/10

Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite

Id	Nombre de tarea	Nombres de los recursos	Entregables	Duración
102	A.- Generar la matriz de impacto e indicar de qué manera cada caso afecta a la CNSF	Antonio Guevara,Jorge	43. Documento de Matriz de Impacto.	20 días
103	**g. Análisis de estrategias posibles de recuperación**			**1 día**
104	A.- Generar propuestas de estrategias de recuperación de acuerdo a los resultados obtenidos	Antonio Guevara,Jorge	44. Documento con el Listado de	1 día
105	**h. Desarrollo de estrategias de recuperación**			**1 día**
106	A.- Depurar en conjunto con el personal de la CNSF las estrategias propuestas para los escenarios de	Antonio Guevara,Jorge	45. Documento con el Listado de	1 día
107	**i. Desarrollo de BIA**			**20 días**
108	A.- Desarrollar el Análisis de Impacto al Negocio.	Antonio Guevara,Jorge	46. Documento de Análisis de Impacto	20 días
109	PROGRAMA V. PROGRAMAs del SGSI: Verificar			**23 días**
110	**Proyecto I.- Revisiones Independientes**			**2.5 días**
111	A.- Realizar un reporte con observaciones acerca de la efectividad, funcionamiento y	Mario Ureña,Jorge	47. Documento de Reporte de Auditoría	2.5 días
112	**Proyecto II.- Desarrollo de Procedimiento de Auditorías internas**			**5 días**
113	A.- Revisar y actualizar el procedimiento de auditoría interna.	Mario Ureña	48. Procedimiento de Auditoría Interna	5 días
114	A.- Acompañamiento del proveedor al equipo de auditoría de la DGI durante la primera auditoría	Mario Ureña,Jorge		2.5 días
115	**Proyecto III.- Revisión de la política**			**2.5 días**
116	A.- Revisión y actualización de la documentación anexa a la política de Seguridad de la	Mario Ureña,Beatriz	49. Política de Seguridad de la	2.5 días
117	**Proyecto IV.- Evaluación de Riesgos Residuales**			**15 días**
118	A.- De acuerdo a las estrategias de mitigación recomendadas, se deberá obtener un aproximado del	Jorge Lozano,Mario	50. Entregar un aproximado del	15 días
119	A.- Desarrollar la carta de aceptación de riesgo residual de la DGI.	Comité de Seguridad de la	51.Carta de aceptación de riesgo	2 días
120	**Proyecto V.- Desarrollo de Procedimiento de Administración y monitoreo de Incidentes del SGSI**			**23 días**



Proyecto: Proyect1- test
Fecha: jue 22/07/10

Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite

Id	Nombre de tarea	Nombres de los recursos	Entregables	Duración
121	A.- Desarrollar, detallar y documentar el procedimiento de administración y monitoreo de incidentes del SGSI.	Antonio Guevara,Raúl	53. Procedimiento para el manejo,	23 días
122	PROGRAMA VI. PROGRAMAs del SGSI: Actuar			**2 días**
123	**Proyecto I.- Revisión de Procedimiento de Acciones Correctivas y Preventivas del SGSI**			**2 días**
124	A.- Desarrollar, detallar y documentar el procedimiento de administración y monitoreo de incidentes del SGSI.	Comité de Seguridad de la	54. Procedimiento para el manejo,	2 días
125	PROGRAMA VII. Definir y ejecutar el plan de entrenamiento y concientización			**21 días**
126	**Proyecto I.- Análisis de Audiencias y Desarrollo de temario y alcance**			**3 días**
127	A.- Evaluar los conocimientos de Seguridad de la Información del personal de la DGI.	SecureInformation Chio,Guillermo	55. Listado de grupos del personal	3 días
128	A.- Armar grupos del personal de la DGI de acuerdo a los conocimientos.	SecureInformation Chio,Guillermo		3 días
129	A.- Desarrollar el temario y alcance de la concientización del personal de la DGI.	SecureInformation Chio,Guillermo	56. Documento de Temario y alcance de	3 días
130	**Proyecto II.- Diseñar, Desarrollar e Implementar la Campaña de Concientización**			**9 días**
131	A.- Impartir los cursos de concientización.	Mario Ureña,Jorge	57. Materiales expuestos 58. Listas	9 días
132	A.- Realizar la difusión de los materiales preparados.	SecureInformation Chio,Guillermo		3 días
133	**Proyecto III.- Medición de la efectividad de la campaña**			**5 días**
134	A.- Realizar evaluaciones al final de cada curso para medir la efectividad del mismo.	SecureInformation Chio,Guillermo	59. Resultados de las evaluaciones de	3 días
135	A.- Realizar encuestas entre el personal para evaluar la efectividad de los medios alternos utilizados.	SecureInformation Chio,Guillermo	60. Resultados de las encuestas de los	3 días
136	PROGRAMA VIII. Cierre del proyecto			**5 días**
137	Verificar que todas las actividades se hayan dado por terminadas.	Comité de Seguridad de la	61. Carta de formalización de uso	5 días
138	Formalizar el cierre del proyecto.	Comité de Seguridad de la		5 días
139	Desarrollar una carta de formalización de uso del SGSI.	Fernando Olvera; Raúl Chio		3 días

Proyecto: Proyect1- test
Fecha: jue 22/07/10

Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite

Id		Nombre de tarea	Nombres de los recursos	Entregables	Duración	tri 3 2009			tri 4 2009		
						jul	ago	sep	oct	nov	dic
140		Desarrollar una carta de cierre del proyecto.	Comité de Seguridad de la	62. Carta de cierre del proyecto.	3 días						Com

Proyecto: Proyect1- test
Fecha: jue 22/07/10

Tarea
División
Progreso
Hito
Resumen
Resumen del proyecto
Tareas externas
Hito externo
Fecha límite

DIRECCION GENERAL DE INFORMATICA

SUBDIRECCION DE RECURSOS INFORMATICOS

DEPARTAMENTO DE SOPORTE ADMINISTRATIVO

SERVICIOS DGI-H

ENERO DEL 2008

AREA	NUMERO SOLICITUD	TIPO DE SERVICIO				FUNCIONARIO	DESCRIPCION	FECHA RECEPCION	ENTREGADO A:	FECHA TERMINO
		S.T.H.	S.T.S.	A.S.	A.P.					
D.G.J.C.C.I.	1		X			Emilia Caballero	Problemas con el sistema de despacho.	03/01/2008	JM	03/01/2008
D.G.S.P.	2		X			Alicia Altamirano	Fallas en Office.	03/01/2005	TTR	03/01/2008
D.G.D.I	3		X			Sergio Venegas	No puede accesar a una carpeta.	03/01/2005	TTR	03/01/2008
D.G.S.A.	4		X			Óscar Aranda	Mensaje de intromisión de chasis.	04/01/2005	TTR	
D.G.S.A.	5		X			Gabriel Cárdenas	Escaneo de 164 hojas.	04/01/2005	TTR	05/01/2008
Presidencia	6				X	Manuel Aguilera	Cañón y lap top en sala de junta de gobierno, día 7 a las 10:30 hrs.	04/01/2005	TTR	07/01/2008
D.G.D.I	7				X	Ricardo Sevilla	Cañón en el auditorio, día 10 a las 11 hrs.	04/01/2005	TTR	CANCELADO
D.G.D.I	8				X	Ricardo Sevilla	Cañón en el auditorio, día 17 a las 11 hrs.	04/01/2005	TTR	17/01/2008
D.G.S.R.	9				X	Jorge L. Ponce	Lap top en el auditorio, día 7 a las 9 hrs.	04/01/2005	TTR	07/01/2008
D.G.S.R.	10				X	Jorge L. Ponce	Lap top en el auditorio, día 12 a las 9:15 hrs.	04/01/2005	TTR	12/01/2008
D.G.S.R.	11				X	Jorge L. Ponce	Lap top en el auditorio, día 13 a las 9:15 hrs.	04/01/2005	TTR	13/01/2008
D.G.S.A.	12		X			Salvador Monroy	Acceso a la unidad "Y".	04/01/2005	UHM	
D.G.D.I	13				X	Ricardo Sevilla	Cañón en el auditorio, día 14 a las 11 hrs.	04/01/2005	TTR	14/01/2008
D.G.J.C.S.	14		X			Víctor Galindo	Problemas con el control de gestión.	05/01/2005	JM	05/01/2008
D.G.S.R.	15		X			Mónica García	Reinstalar antivirus.	05/01/2005	TTR	05/01/2008
D.G.J.C.S.	16		X			César Romero	No puede imprimir desde el sistema de despacho.	05/01/2005	JM	05/01/2008
D.G.J.C.C.I.	17	X				Óscar Limón	Diskette atorado.	05/01/2005	TTR	05/01/2008
D.G.J.C.S.	18		X			Pilar Jiménez	Acceso al módulo de observaciones a agentes.	05/01/2005	MAB	06/01/2008
D.G.J.C.C.I.	19	X				Teresa Chávez	No respalda su no-break.	05/01/2005	TTR	10/01/2008
D.G.J.C.C.I.	20	X				Jorge Trevisan	No respalda su no-break.	05/01/2005	TTR	05/01/2008
D.G.J.C.S.	21	X				Diana Rodríguez	Falla en impresora.	06/01/2005	TTR	06/01/2008
D.G.A.	22	X				Ramón Blancas	No respalda su no-break.	06/01/2005	TTR	06/01/2008
D.G.J.C.C.I.	23		X			Paula Enriquez	No funciona su reproductor de Windows Media.	06/01/2005	TTR	12/01/2008
D.G.A.	24	X				Maricela Zepeda	No respalda su no-break.	06/01/2005	TTR	
D.G.S.P.	25	X				Alejandro Ramos	No respalda su no-break.	06/01/2005	TTR	07/01/2008
D.G.J.C.S.	26		X			Alejandra Méndez	Problemas con el sistema de despacho.	06/01/2005	JM	06/01/2008

DIRECCION GENERAL DE INFORMATICA

SUBDIRECCION DE RECURSOS INFORMATICOS

DEPARTAMENTO DE SOPORTE ADMINISTRATIVO

SERVICIOS DGI-H

ENERO DEL 2008

AREA	NUMERO SOLICITUD	TIPO DE SERVICIO				FUNCIONARIO	DESCRIPCION	FECHA RECEPCION	ENTREGADO A:	FECHA TERMINO
		S.T.H.	S.T.S.	A.S.	A.P.					
D.G.S.A.	27		X			Héctor Quiroz	Perdió un acceso directo.	07/01/2005	TTR	07/01/2008
D.G.D.I	28			X		Sergio Venegas	Asesoría para compartir carpetas.	07/01/2005	TTR	07/01/2008
Presidencia	29				X	Manuel Aguilera	Cañón y lap top en sala de junta de gobierno, los días 11 y 12 a las 17 hrs.	07/01/2005	TTR	11/01/2008
Presidencia	30				X	Manuel Aguilera	Cañón y lap top en sala de junta de gobierno, día 11 a las 18:45 hrs.	07/01/2005	TTR	11/01/2008
D.G.S.F.	31		X			Sául Macías	Instalación del SAEF.	07/01/2005	TNS	07/01/2008
D.G.S.A.	32		X			Héctor Quiroz	No accesa a la unidad "Y".	07/01/2005	ATM	
D.G.D.I	33		X			Sergio Venegas	No accesa a la unidad "T".	07/01/2005	TNS	07/01/2008
D.G.J.C.S.	34		X			Óscar Mendoza	No accesa al sistema de agentes.	07/01/2005	MAB	10/01/2008
D.G.S.A.	35				X	Ulises Rubio	Cañón en sala de junta de gobierno, día 10 a las 11 hrs.	07/01/2005	TTR	10/01/2008
D.G.J.C.S.	36	X				Diana Rodríguez	Su impresora no jala las hojas.	10/01/2005	TTR	10/01/2008
D.G.A.	37	X				Carlos Cotero	No respalda su no-break.	10/01/2005	TTR	
D.G.D.I	38		X			Lourdes Oviedo	No puede accesar a red.	10/01/2005	TTR	10/01/2008
D.G.S.S.	39		X			Guadalpe Castañeda	No puede accesar a red.	10/01/2005	ATM	
D.G.J.C.C.I.	40		X			Lourdes Cervantes	No puede accesar a red.	10/01/2005	TTR	10/01/2008
D.G.J.C.C.I.	41	X				Paula Enriquez	No respalda su no-break.	10/01/2005	TTR	
D.G.S.S.	42		X			Alejandra Méndez	Problemas con el sistema de despacho.	10/01/2005	HJL	10/01/2008
Veracruz	43		X			Rosa Arce	No puede enviar mails.	10/01/2005	HJL	
D.G.S.F.	44		X			Patricia de la Teja	Problemas con el sistema de despacho.	10/01/2005	HJL	10/01/2008
D.G.A.	45		X			Hugo Hernández	Recuperar un mail de octubre del 2004.	10/01/2005	JM	11/01/2008
D.G.S.R.	46		X			Alberto Rivera	No accesa a lotus.	10/01/2005	ATM	
D.G.J.C.S.	47		X			Víctor Galindo	Falla en impresora.	10/01/2005	TTR	10/01/2008
D.G.S.P.	48	X				Héctor Rodríguez	No respalda su no-break.	11/01/2005	TTR	11/01/2008
D.G.A.	49		X			Luz Varea	Instalación del sistema de servicio médico.	11/01/2005	TNS	
D.G.S.S.	50		X			Carlos Ravelo	No accesa a lotus.	11/01/2005	JM	11/01/2008
D.G.S.F.	51		X			Patricia de la Teja	Problemas con el sistema de despacho.	11/01/2005	HJL	12/01/2008
D.G.A.	52	X				Edith Vergara	Traslado de equipo.	11/01/2005	TTR	14/01/2008
D.G.S.A.	53	X				Carolina Gómez	No respalda su no-break.	11/01/2005	TTR	11/01/2008
D.G.J.C.S.	54	X				Bertha Chavero	Falla en impresora.	11/01/2005	TTR	11/01/2008

DIRECCION GENERAL DE INFORMATICA

SUBDIRECCION DE RECURSOS INFORMATICOS

DEPARTAMENTO DE SOPORTE ADMINISTRATIVO

SERVICIOS DGI-H

ENERO DEL 2008

AREA	NUMERO SOLICITUD	TIPO DE SERVICIO				FUNCIONARIO	DESCRIPCION	FECHA RECEPCION	ENTREGADO A:	FECHA TERMINO
		S.T.H.	S.T.S.	A.S.	A.P.					
D.G.S.F.	55		X			Luz Ma. Flores	Configurar impresora.	11/01/2005	TTR	11/01/2008
D.G.J.C.C.I.	56		X			Óscar Limón	No puede imprimir desde Acrobat.	11/01/2005	TTR	11/01/2008
D.G.J.C.C.I.	57		X			Maribel Flores	Falla en impresora.	11/01/2005	TTR	11/01/2008
D.G.A.	58		X			Martha Tovar	Volcado físico ce memoria.	12/01/2005	TTR	12/01/2008
D.G.A.	59	X				Elizabeth Cabello	Papel atorado.	12/01/2005	TTR	12/01/2008
D.G.J.C.S.	60	X				César Romero	No respalda su no-break.	12/01/2005	TTR	01/02/2008
D.G.D.I	61		X			Consuelo Anzures	No imprime correctamento los sellos.	12/01/2005	JM	12/01/2008
D.G.S.R.	62		X			Alberto Rivera	Falla en lap top.	13/01/2005	TTR	13/01/2008
D.G.S.F.	63	X				Lorena Cruz	No respalda su no-break.	13/01/2005	TTR	
D.G.J.C.S.	64		X			Pilar Jiménez	Instalación del "Control de Sanciones".	13/01/2005	UHM	
D.G.J.C.S.	65	X				Diana Rodríguez	Falla en impresora.	13/01/2005	TTR	13/01/2008
D.G.S.S.	66				X	Fernando Vanegas	Lap top en sala de junta de gobierno, día 14 a las 12:30 hrs.	13/01/2005	TTR	CANCELADO
D.G.S.F.	67		X			Sonia Tavera	No accesa a SIIF.	13/01/2005	VM	17/01/2008
D.G.J.C.S.	68	X				Ranferi Gómez	Falla en impresora.	13/01/2005	TTR	CANCELADO
D.G.S.R.	69		X			Alberto Rivera	No accesa al SUI.	13/01/2005	TNS	
D.G.A.	70		X			Martha Tovar	No inicialliza su PC.	14/01/2005	TTR	14/01/2008
C.I.	71		X			Rosa Ma. Sánchez	Va a expirar su certificación de Lotus.	14/01/2005	JM	
D.G.J.C.C.I.	72		X			Óscar Limón	Problemas con el sistema de despacho.	14/01/2005	HJL	17/01/2008
V.J.	73				X	Víctor González	Cañón y lap top en sala de junta de gobierno, día 17 a las 17 hrs.	14/01/2005	TTR	17/01/2008
D.G.S.P.	74		X			Carolina López	No se conecta al SIIF.	17/01/2005	VM	17/01/2008
D.G.A.	75	X				Edith Vergara	No respalda su no-break.	17/01/2005	TTR	17/01/2008
D.G.S.F.	76		X			Marino Hernández	No puede imprimir en red.	17/01/2005	TTR	17/01/2008
D.G.S.S.	77		X			Fernando Vanegas	Dar de alta impresora en red.	17/01/2005	TTR	17/01/2008
D.G.S.F.	78		X			Fernando Pérez	Mensaje de error en Módulos de Explotación.	17/01/2005	VM	18/01/2008
D.G.S.A.	79		X			Laura G. Lozada	No se conecta al SIIF.	17/01/2005	VM	17/01/2008
D.G.A.	80		X			Ernesto Bravo	No accesa a lotus.	17/01/2005	ATM	
D.G.S.A.	81		X			Rosario Vega	Va a expirar su certificación de Lotus.	18/01/2005	JM	21/01/2008
D.G.A.	82	X				Magda Alcántar	Falta cable de corriente para el no-break	18/01/2005	TTR	18/01/2008

DIRECCION GENERAL DE INFORMATICA

SUBDIRECCION DE RECURSOS INFORMATICOS

DEPARTAMENTO DE SOPORTE ADMINISTRATIVO

SERVICIOS DGI-H

ENERO DEL 2008

AREA	NUMERO SOLICITUD	TIPO DE SERVICIO				FUNCIONARIO	DESCRIPCION	FECHA RECEPCION	ENTREGADO A:	FECHA TERMINO
		S.T.H.	S.T.S.	A.S.	A.P.					
D.G.S.A.	83				X	Ulises Rubio	Paleta de cuarzo en sala de juntas 1er. Piso torre sur, día 18 a las 10:30 hrs.	18/01/2005	TTR	18/01/2008
D.G.J.C.C.I.	84		X			Lucas Ginez	No inicialliza su PC.	18/01/2005	TTR	18/01/2008
D.G.S.A.	85				X	Ulises Rubio	Paleta de cuarzo en sala de juntas 1er. Piso torre sur, día 18 a las 16:00 hrs.	18/01/2005	TTR	18/01/2008
D.G.I.	86				X	Guillermo Orozco	Cañón y lap top en sala de junta de gobierno, día 20 a las 17 hrs.	18/01/2005	TTR	20/01/2008
D.G.A.	87		X			Martín Enrique Pérez Thompson	Personalizar su equipo.	18/01/2005	JM	19/01/2008
D.G.S.F.	88		X			Verónica Castro	Personalizar su equipo.	18/01/2005	VM	20/01/2008
D.G.S.F.	89		X			Patricia de la Teja	Asesoría con SIIF.	18/01/2005	VM	19/01/2008
D.G.J.C.C.I.	90		X			Heryeirejeus Velazco	No puede imprimir en red.	18/01/2005	TTR	18/01/2008
D.G.S.F.	91		X			Gustavo Rosas García	Personalizar su equipo.	18/01/2005	MAB	21/01/2008
V.J.	92	X				Víctor González	No respalda su no-break.	18/01/2005	TTR	18/01/2008
D.G.A.	93	X				Martha Tovar	Se trabó su impresora.	18/01/2005	TTR	18/01/2008
D.G.J.C.C.I.	94		X			Teresa Chávez	Conflicto en dirección IP.	18/01/2005	TTR	18/01/2008
D.G.J.C.C.I.	95		X			Yazmín Cabrera	Problemas con la dirección electrónica "Vicepresidencia Jurídica".	18/01/2005	JM	19/01/2008
D.G.J.C.S.	96	X				Bertha Chavero	No respalda su no-break.	19/01/2005	TTR	19/01/2008
D.G.S.F.	97		X			Daniela González	Personalizar su equipo.	20/01/2005	TTR	20/01/2008
D.G.S.F.	98		X			Miriam Rodríguez	Personalizar su equipo.	20/01/2005	TNS	21/01/2008
D.G.J.C.C.I.	99		X			Marcela Espinoza	No puede activar el traductor desde Intranet.	20/01/2005	ATM	
D.G.D.I	100		X			Consuelo Anzures	No accesa al sistema de vacaciones.	20/01/2005	VM	20/01/2008
V.O.I.	101				X	Manuel Calderón	Cañón y lap top en sala de junta de gobierno, día 21 a las 10 hrs.	20/01/2008	TTR	21/01/2008
Presidencia	102				X	Hugo Fernández	Cañón en sala de junta de gobierno, día 3 de febrero a las 12 hrs.	20/01/2005	TTR	03/02/2008
D.G.J.C.S.	103		X			Diana Rodríguez	Falla en impresora.	20/01/2005	TTR	20/01/2008
D.G.I.	104				X	Tirso Nava	Canón en sala de juntas de la DGI, día 25 a las 13 hrs.	20/01/2005	TTR	25/01/2008

DIRECCION GENERAL DE INFORMATICA

SUBDIRECCION DE RECURSOS INFORMATICOS

DEPARTAMENTO DE SOPORTE ADMINISTRATIVO

SERVICIOS DGI-H

ENERO DEL 2008

AREA	NUMERO SOLICITUD	TIPO DE SERVICIO				FUNCIONARIO	DESCRIPCION	FECHA RECEPCION	ENTREGADO A:	FECHA TERMINO
		S.T.H.	S.T.S.	A.S.	A.P.					
Guadalajara	105		X			Rafael Coello	Falla en impresora.	20/01/2005	TTR	31/01/2008
D.G.S.F.	106		X			Daniela González	Acceso al SIE, SIIF y SAEF.	21/01/2005	MAB	25/01/2008
D.G.J.C.C.I.	107		X			Eligia Santacruz	Problemas con el sistema de despacho.	21/01/2005	JM	21/01/2008
C.I.	108				X	Susana Parra	Cañón y lap top en sala de junta de gobierno, día 10 a las 9 hrs.	21/01/2005	TTR	10/02/2008
Guadalajara	109		X			Rafael Coello	Clave de acceso al sistema de agentes para Eduardo F. Rodríguez Hernández.	21/01/2005	MFM	24/01/2008
D.G.D.I	110			X		Sergio Venegas	Asesoría para descompactar un archivo.	21/01/2005	TNS	21/01/2008
D.G.S.S.	111		X			Carlos Ravelo	No accesa al SIE.	21/01/2005	TNS	
D.G.S.P.	112		X			Hazael López	Instalación de PROJECT.	21/01/2005	GOG	CANCELADO
Presidencia	113				X	Hugo Fernández	Cañón y lap top en sala de junta de gobierno, día 24 a las 12 hrs.	21/01/2005	TTR	24/01/2008
D.G.J.C.C.I.	114		X			Teresa Chávez	Error en lotus.	21/01/2005	JM	21/01/2008
C.I.	115		X			Dulce González	Personalizar su equipo.	24/01/2005	TTR	24/01/2008
D.G.S.F.	116			X		Verónica Castro	Asesoría SIIF.	24/01/2005	TNS	24/01/2008
D.G.S.F.	117		X			Miriam Rodríguez	Acceso a "L".	24/01/2005	ATM	
D.G.A.	118		X			Maricela Zepeda	Falla en impresora.	24/01/2005	TTR	25/01/2008
D.G.S.F.	119		X			Blanca Martínez	Personalizar su equipo.	24/01/2005	TTR	24/01/2008
D.G.J.C.C.I.	120		X			Heryeirejeus Velazco	No puede imprimir en red.	24/01/2005	TTR	24/01/2008
D.G.S.F.	121		X			Blanca Martínez	No accesa al SIE, SIIF y SUI.	24/01/2005	MAB	24/01/2008
D.G.S.A.	122		X			Ángeles Arellano	Error en Excel.	24/01/2005	TTR	24/01/2008
D.G.S.A.	123		X			Laura G. Lozada	No accesa al SIIF.	24/01/2005	MAB	25/01/2008
D.G.S.A.	124		X			Gabriel Cárdenas	No accesa a la red.	24/01/2005	TTR	
D.G.S.F.	125		X			Daniela González	Acceso a la base de datos de SIGAEF.	25/01/2005	TNS	CANCELADO
D.G.S.F.	126		X			Miriam Rodríguez	Instalación del PREPA.	25/01/2005	JM	25/01/2008
D.G.S.F.	127	X				Rebeca Pérez	Solicita cambio de equipo para Daniela González y Blanca Martínez.	25/01/2005	MMB	CANCELADO
D.G.I.	128				X	Tirso Nava	Cañón en sala de juntas D.G.I., día 27 a las 10 hrs.	25/01/2005	TTR	27/01/2008
D.G.A.	129				X	Edith Vergara	Lap top en el auditorio, días 8, 9 y 10 de junio a las 9 hrs.	25/01/2005	TTR	07/06/2008