INSTITUTO POLITÉCNICO NACIONAL

SECRETARIA DE INVESTIGACION Y POSGRADO

CENTRO DE INVESTIGACIONES ECONOMICAS, ADMINISTRATIVAS Y SOCIALES

"LA GESTIÓN DEL CAMBIO TECNOLÓGICO DE LA SEGURIDAD INFORMÁTICA EN EL IPN: LA DIRECCIÓN DE CÓMPUTO Y COMUNICACIONES (DCYC) COMO CASO DE ESTUDIO"

TESIS

QUE PARA OBTENER EL GRADO DE:
MAESTRO EN POLÍTICA Y GESTIÓN DEL CAMBIO TECNOLÓGICO
PRESENTA:

Ing. Alejandro Hércules Arellano Luján

Director de Tesis:

Dr. Humberto Merritt Tapia

México D.F. noviembre de 2011

SIP-14

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

ACTA DE REVISIÓN DE TESIS

En la Ciudad de México D.F. siendo las 16:00 horas del día 23 del mes de Noviembre del 2011 se reunieron los miembros de la Comisión Revisora de la Tesis, designada por el Colegio de Profesores de Estudios de Posgrado e Investigación de CIECAS para examinar la tesis titulada:

"Gestión del cambio tecnológico de la seguridad informática en el IPN: Caso de estudio, Dirección de Cómputo y Comunicación (DCYC)"

Presentada por el alumno:

Arellano	Luján	Alejandro Hércules
Apellido paterno	Apellido materno	Nombre(s)

Con registro: B 0 8 2 0 0 1

aspirante de:

Maestría en Política y Gestión del Cambio Tecnológico

Después de intercambiar opiniones, los miembros de la Comisión manifestaron ***APROBAR LA TESIS***, en virtud de que satisface los requisitos señalados por las disposiciones reglamentarias vigentes.

LA COMISIÓN REVISORA

Director(a) de tesis

Dr. Humberto Merritt Tapia

Dra. Hortensia Gómez Víquez

M. en E. Pedro Mendoza Acosta

M. en C. Octavio Augusto Palacios Sommer

Dr. José Benjamín Méndez Bahena

PRESIDENTE DEL COLEGIO DE PROFESORES

Dr. Zacarías Torres Hernández

SECRETARIA DE EDUCACION PUBLICA
INSTITUTO POLITECNICO NACIONAL
CENTRO DE INVESTIGACIONES
ECONOMICAS ADMINISTRATIVAS

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA DE INVESTIGACIÓN Y POSGRADO

CARTA CESIÓN DE DERECHOS

En la Ciudad de México el día 23 del mes de Noviembre del año 2011, el (la) que suscribe Alejandro Hércules Arellano Luján alumno (a) del Programa de Maestría en Política y Gestión del Cambio Tecnológico con número de registro B082001, adscrito al Centro de Investigaciones Económicas, Administrativas y Sociales, manifiesta que es autor (a) intelectual del presente trabajo de Tesis bajo la dirección del Humberto Merritt Tapia y cede los derechos del trabajo intitulado: La gestión del cambio tecnológico de la seguridad informática en el IPN: La Dirección de Cómputo y Comunicaciones (DCyC) como caso de estudio, al Instituto Politécnico Nacional para su difusión, con fines académicos y de investigación.

Los usuarios de la información no deben reproducir el contenido textual, gráficas o datos del trabajo sin el permiso expreso del autor y/o director del trabajo. Este puede ser obtenido escribiendo a la siguiente dirección aarellan@ipn.mx. Si el permiso se otorga, el usuario deberá dar el agradecimiento correspondiente y citar la fuente del mismo.

Nombre y firma

DEDICATORIA

El presente trabajo de tesis está dedicado a mi familia: Mi esposa Jane Austria Navarrete por su entusiasmo en buscar apoyos, a mis Padres: Mario Arellano Herrera y Luz María Luján Suárez por su ardua tarea de ser guías, motivadores y ejemplos a seguir y a mis hermanos Juan, Luz María, Héctor, Mario y Paola por su apoyo y motivación.

Como también a todos aquellos que formamos parte de una pequeña y especial comunidad de compañeros y Maestros que con gran esmero motivaron reflexiones profesionales de toda índole enriqueciendo el contenido académico de los cursos durante estos 2 años y medio de esfuerzo, sin esta asociación y teniendo como puntal la experiencia de los Maestros pude llevar a buen término la tarea emprendida.

AGRADECIMIENTOS

Al INSTITUTO POLITÉCNICO NACIONAL por permitirme desarrollar de forma integral como estudiante, profesional y ciudadano.

A la Dra. Hortensia Gómez Víquez por su gran empeño en sacar adelante a la generación 2008-2010 de Maestros en Política y Gestión del Cambio Tecnológico.

A todos y cada uno de los profesores que participaron en el Programa de Maestría por sus enseñanzas, comprensión y correcciones en mis inconsistencias.

A aquellos que como seres queridos familiares o no compartieron y comprendieron mi aspiración de superación y progreso académico.

Al Dr. Humberto Merritt Tapia por su apoyo, empatía, paciencia, correcciones y aportaciones estructurales del presente trabajo bajo su dirección.

Al Ing. Martín Haro Martínez Coordinador General de Servicios Informáticos del IPN por el interés a desarrollar el tema mediante la aportación de información y datos técnicos fundamentales en la presente investigación.

A los Mtros. Jaime González Amaro y Netzahualcóyotl Flores Rodríguez de la Dirección de Informática del IEDF y al Lic. Octavio Domínguez Romero Director de Servicios Informáticos de la CMHALDF por su interés y aportaciones técnicas que enriquecieron el presente trabajo.

Al Mtro. Francisco Platas López Director de Alarmas Nacionales SSP por el tiempo invertido en leer el presente trabajo sus aportaciones y correcciones.

A Jane Austria Navarrete y la Fundación Telmex por su motivación para obtener el apoyo como su becario.

RESUMEN

La presente tesis revisa la situación actual que guardan las políticas de seguridad informática mayormente aplicadas en México. Posteriormente se hace un diagnostico sobre la gestión del cambio tecnológico en el área de seguridad informática del Instituto Politécnico Nacional (IPN). Para ello, Se considera como caso de estudio la Dirección de Cómputo y Comunicaciones (DCYC) del IPN.

Las políticas para la gestión de los riesgos informáticos en el Instituto Politécnico Nacional están contempladas con la Ley Orgánica del instituto y en su reglamento interno, los cuales fijan las reglas, controles y procedimientos para estandarizar la forma en que el instituto previene, protege y mitiga los riesgos de seguridad en las distintas instancias de operación. Sin embargo, para una correcta implementación de mecanismos de gestión del riesgo informático en el IPN se requieren cambios organizacionales que acepten, e incluso agilicen, la adopción de elementos enfocados a la prevención de los riesgos informáticos. En esta tesis se revisa la situación que guarda la gestión del cambio tecnológico en el área de la seguridad informática en el IPN tomando como referencia el caso de la Dirección de Cómputo y Comunicaciones (DCYC) del IPN. La tesis presenta una serie de recomendaciones derivadas del análisis organizacional de la DCYC destinadas a mejorar la gestión de la seguridad informática en el IPN.

ABSTRACT

This thesis reviews the current situation of the information security policies that are applied in Mexico. It aims at reviewing the management of technological change in the computer security area of the National Polytechnic Institute (IPN). In order to do this, the Department of Computing and Communications (DCYC) of the IPN is used as a case study.

The policies for managing IT risk in the IPN are matters covered by the Organic Law of the Institute and its internal regulations, which set the rules, controls and procedures to standardize how the institute warns, protects and mitigates security risks at all levels of operation. However, in order to have a proper implementation of the mechanisms for information risk management at IPN several organizational changes are required to accept, and even speed up the adoption of elements aimed at the prevention of computer risks. In particular, this thesis reviews the situation of the management of technological change in the area of computer security in the IPN with reference to the DCYC. Finally, the thesis also presents a series of recommendations stemming from the DCYC organizational analysis in order to improve the management of the information security in the IPN.

INDICE

TABLAS y FIGURAS

GLOSARIO

ANTIVIRUS: Es una aplicación, o programa dedicado a detectar y eliminar virus informáticos. La forma en que opera es la siguiente, el sistema de protección del Antivirus depende del sistema operativo en que se esté trabajando. En el sistema DOS se utilizan programas que terminan y se quedan residentes en memoria como TSR (Terminate and Stay Resident). En Windows 95/98 VxD (Virtual Driver) y en NT drivers en modo Kernel.

AUTENTICACIÓN: Es la confirmación de la identidad declarada de los usuarios de un sistema informático. Los Métodos de autenticación adecuados son necesarios para muchos servicios y aplicación es como la conclusión de un contrato en línea, el control del acceso a datos y servicios de cómputo, la autenticación de los sitios web, etc.

AUTORREPLICABLES: Son los virus que realizan las funciones más parecidas a los virus biológicos, ya que se auto rreproducen e infectan los programas ejecutables que se encuentran en el disco. Se activan en una fecha u hora programada o cada determinado tiempo, contado a partir de su última ejecución, o bien cuando se trata de manipular alguno de sus componentes para tratar de detectarlos. Un ejemplo de estos es el virus llamado “viernes 13”, que se ejecuta en esa fecha o se borra (junto con los programas infectados), evitando ser detectado.

BIENES INFORMÁTICOS: Se le denomina así a todo bien material que sirve para satisfacer las necesidades en materia de gestión, procesamiento, almacenamiento, comunicación o distribución de información digital.

BOMBA DE TIEMPO: Son los programas ocultos en la memoria del sistema o en los discos, o en los archivos de programas ejecutables con tipo COM o EXE e n espera de una fecha o una hora determinadas para a c t i v a r s e (explotar). Algunos de estos virus no son destructivos y solo exhiben mensajes en las pantallas al llegar el momento de la "explosión". Llegado el momento se activan cuando se ejecuta el programa que las contiene.

CABALLOS DE TROYA: Son rutinas de cómputo que se introducen al sistema bajo una apariencia totalmente diferente a la de su objetivo final porque se presentan como información perdida o "basura" sin ningún sentido; y al cabo de algún tiempo se activan, mediante una indicación programada, y comienzan a ejecutarse realizando acciones destructivas en el sistema.

Computo en la Nube (CLOUD COMPUTING): Es un nuevo modelo de prestación de servicios de negocio y tecnología que permite al usuario acceder a un catálogo de servicios estandarizados y responder a las necesidades de su negocio, de forma flexible y adaptativa. En caso de que se requieran aplicaciones no previsibles o se presenten picos de trabajo se paga únicamente por el consumo efectuado.

COMITÉ: Comité Institucional de Tecnologías de la Información y las Comunicaciones.

CONFIDENCIALIDAD: Mecanismo de protección de los datos almacenados y/o de las comunicaciones realizadas por los usuarios contra su interceptación y lectura por parte de personas no autorizadas. La confidencialidad es necesaria para la transmisión de datos sensibles y es uno de los requisitos principales a la hora de dar respuesta a las inquietudes en materia de privacidad de los usuarios de las redes de comunicación.

COORDINACIÓN: Coordinación General de Servicios Informáticos del Instituto Politécnico Nacional.

CORREO ELECTRÓNICO (E-MAIL): Sistema de transmisión de información a través de algún canal de comunicaciones electrónico.

DESARROLLO TECNOLÓGICO: Resultado de la aplicación sistemática de conocimientos científicos, tecnológicos y/o de índole práctica que lleva a la generación de prototipos o a una mejora sustantiva a bienes existentes independientemente de su implementación o comercialización inmediata.

DIRECCIÓN IP: Código de identificación numérica de un nodo o servidor en Internet que consta de cuatro números del 0 al 255 separados por puntos.

DISPONIBILIDAD: Significa que los datos son accesibles, inclusive en casos de alteraciones, cortes de energía, fenómenos destructivos de origen natural, accidentes o ataques. Esta característica es particularmente importante cuando una avería de la red puede provocar interrupciones o reacciones en cadena que afecten las operaciones de la empresa.

EQUIPO DE CÓMPUTO: Son los dispositivos eléctricos, electrónicos y mecánicos que se emplean para procesar datos.

GESTIÓN DE LA TECNOLOGÍA: Conocimientos organizados entorno a procesos, métodos y prácticas que actúan sobre la planeación, desarrollo, control, integración y capitalización de los recursos para la implantación de cambios tecnológicos o innovaciones en empresas e instituciones con el propósito de mantener o mejorar la posición competitiva.

GUSANOS (WORM): Son programas de cómputo que se reproducen a sí mismos y no requieren de un anfitrión pues se "arrastran" por todo el sistema sin necesidad de un programa que los transporte. Los gusanos se cargan en la memoria y se posicionan en una determinada dirección, luego se copian en otro lugar y se borran del que ocupaban, y así sucesivamente. Esto hace que queden borrados los programas o la información que encuentran a su paso por la memoria, lo que causa problemas de operación o pérdidas de datos.

HARDWARE: Es el conjunto de dispositivos físicos de los que se compone una unidad central de procesamiento y que comprende componentes tales como la placa madre, el teclado, el ratón, las unidades de disco o el monitor, entre otros.

INFORMÁTICA: Es la tecnología para el tratamiento sistemático y racional de la información mediante el procesamiento electrónico de datos.

INGENIERÍA SOCIAL: Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil".

INTEGRIDAD: Confirmación de que los datos que han sido enviados, recibidos o almacenados son completos y no han sido modificados. La integridad es especialmente importante en relación con la autenticación para la conclusión de contratos o en los casos en los que la exactitud de los datos es crítica

INTERNET: Red mundial formada por la conexión de redes locales, regionales y nacionales que se han ido enlazando con una instancia reguladora, en la que se intercambian datos y se distribuyen tareas de procesamiento.

KERNEL: Núcleo de un software que constituye la parte más importante del sistema operativo.

MARKET PULL: Es la innovación basada en la demanda del mercado que ha sido desarrollada por la función de I+D en respuesta a una necesidad identificada en el mercado.

PHISHING: Es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta, como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria.

PROCESOS: Conjunto de actividades mutuamente relacionadas o que interactúan con un objetivo claro, que combina diversos recursos, practicas de operación y de organización para generar un desarrollo deseado.

PROGRAMA DE CÓMPUTO: Conjunto de instrucciones codificadas que ordenan a la computadora llevar a cabo determinada tarea en un lenguaje de programación y almacenados en formato electrónico.

RED INSTITUCIONAL: Red Institucional de Cómputo y Telecomunicaciones del Instituto Politécnico Nacional. Es el conjunto de equipos interconectados a través de la infraestructura de comunicaciones que posee el propio Instituto destinados a satisfacer las necesidades de sus dependencias.

REDUNDANCIA: Los sistemas redundantes, en ingeniería de cómputo, son aquellos en los que se repiten aquellos datos o hardware de carácter crítico que se quiere asegurar ante los posibles fallos que puedan surgir por su uso continuado.

SEGURIDAD INFORMÁTICA: Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente pueden involucrarse otras propiedades, tales como autenticidad, responsabilidad, no repudio y confiabilidad basadas en las normas ISO/IEC 17799:2005.

SOFTWARE: Conjunto de instrucciones mediante las cuales una computadora puede realizar las tareas ordenadas por el usuario y que está integrado por los programas, sistemas operativos y utilidades.

TECHNOLOGY PUSH: Término para denotar que un invento (o innovación) es generado por la oferta a través de I+D y las ventas sin que exista una intención explícita de satisfacer una necesidad del mercado.

TECNOLOGÍA: Grado de obtención del valor potencial de un recurso, mediante conocimientos y habilidades relativas al saber hacer y su combinación con recursos materiales de manera sistemática, repetible y reproducible.

TELECOMUNICACIONES: Toda emisión, transmisión o recepción de signos, señales, escritos, imágenes, voz, sonidos o información de cualquier naturaleza que se efectúa a través de hilos, radio-electricidad, medios ópticos, físicos u otros sistemas electromagnéticos.

TELECONFERENCIA: Sistema que permite conversar con una o varias personas simultáneamente, viendo su imagen en movimiento además de la voz.

USUARIO: Todo miembro de la comunidad politécnica que tiene acceso a la Red Institucional por las funciones o actividades que desempeña.

VIDEO CONFERENCIA: Transmisión en la cual las personas se ven unas a otras comunicándose e interactuando al mismo tiempo mediante cámaras y

Monitores de videos ubicados en las instalaciones del cliente o en un centro de video conferencias público.

VIRUS: Programa de cómputo en el que una secuencia de instrucciones y rutinas creadas tiene el único objetivo de alterar el correcto funcionamiento del sistema y que en la inmensa mayoría de los casos corrompe o destruye una parte, o la totalidad, de los datos almacenados en el hardware.

VIRUS DE MACROS/CÓDIGO FUENTE: Son rutinas de programas que se adjuntan a los programas fuente de los usuarios y a las macros utilizadas por Procesadores de Palabras (Word, Works, WordPerfect) u Hoja de Cálculo (Excel, Quattro, Lotus).

VIRUS MUTANTES: Son virus informáticos que al infectar realizan modificaciones a su código, para evitar ser detectados o eliminados. Ejemplos de ello son: NATAS (o SATÁN), Miguel Ángel, Conficker, etc.

ACRÓNIMOS

CIO: Chief Information Officer, Director de seguridad de la Información.

DCYC: Dirección de Cómputo y Comunicaciones del IPN.

DDoS: Negación de servicios distribuido.

DoS: Negación de Servicios.

DOS: Sistema de operación de disco. Familia de sistemas operativos para PC.

I+D: Investigación + Desarrollo.

ISO/IEC 17799:2005: ISO (la Organización Internacional de Estandarización) e IEC (la Comisión Electrotécnica Internacional) Código para la práctica de la gestión de la seguridad de la información. Mejores Prácticas.

ISO/IEC 27000: En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO 27001. Auditable.

IPN: Instituto Politécnico Nacional.

NT: En sistemas operativos Windows Nueva Tecnología.

RFC: Request for Comments ("Petición de Comentarios") son una serie de notas sobre Internet que comenzaron a publicarse en 1969. Cada una de ellas individualmente es un documento cuyo contenido es una propuesta oficial para un nuevo protocolo de la red Internet (originalmente de ARPANET), que se explica con todo detalle para que en caso de ser aceptado pueda ser implementado sin ambigüedades.

TIC: Tecnologías de la Información y la Comunicación.

TSR: Virus Termina y Permanece Residente forma primitiva de multitarea en sistemas DOS.

SGSI: Sistema de Gestión de Seguridad Informática

UDI: Unidades de Informática de las dependencias del IPN.

VxD: En sistemas operativos Windows se refiere a un controlador de dispositivos virtual.

INTRODUCCIÓN

En el actual entorno económico ya no sólo es suficiente contar con la información correcta, sino que también es necesario adelantarse a los requerimientos organizacionales e institucionales. Los directivos de muchas organizaciones, tanto públicas como privadas, están continuamente buscando nuevas herramientas que les ayuden a tomar las decisiones correctas de manera ágil y expedita. Una de estas herramientas son las denominadas Tecnologías de la Información y las Comunicaciones (TIC), dado que el manejo de la información es la clave del éxito (Solleiro y Castañon, 2008). Sin embargo, la calidad y disponibilidad de la información depende críticamente de los sistemas que la administran, almacenan, depuran, gestionan y distribuyen (Anderson, 1980). En los últimos años este tipo de sistemas de administración de la información se han convertido en la columna vertebral de las organizaciones de clase mundial (Jorgenson y Wessner, 2006). Debido al crecimiento en los volúmenes de información y en la sofisticación de los sistemas de administración informáticos, la protección de los mismos ha empezado a cobrar mucha relevancia en vista de la aparición de ataques dirigidos a dichos sistemas, fenómeno que se ha recrudecido en todo el mundo (Ortega, 2010).

En México la cultura de protección a los datos digitales es aún incipiente. Por esta razón muchas instituciones, tanto públicas como privadas, no han buscado desarrollar planes para fomentar de manera sistemática y decidida la gestión de la seguridad informática. Sí la solución a este problema es impostergable en el caso de las grandes corporaciones, en el caso de las instituciones educativas se vuelve crítica la instrumentación de sistemas de gestión de la seguridad informática dada la gran cantidad de usuarios que conforman las comunidades universitarias y que al gestionar los servicios informáticos dependen de manera creciente de su confiabilidad y eficiencia. Así, en los casos en los que se han presentado eventos de disrupción por ataques malintencionados a las redes institucionales, la falta de mecanismos rápidos y efectivos de gestión para el manejo de riesgos informáticos se hace más evidente.

Esto hace que se exhiba la vulnerabilidad inherente de dichos sistemas en el manejo de las diferentes aplicaciones informáticas que se requieren para el desempeño de las

actividades académicas, profesionales y de investigación.

Aunque México se encuentra entre los cinco países de América Latina con mejores niveles de seguridad informática, este tipo de acciones preventivas apenas comienzan a instrumentarse en las instituciones de educación superior del país[1]. En el caso del Instituto Politécnico Nacional (IPN) es indispensable la instrumentación de una práctica tecnológica que se encuentre alineada a un Plan Estratégico Institucional en donde la seguridad de la infraestructura informática se transforme en una política explícita de gestión del riesgo y de la seguridad de la información, y que además sea uno de sus ejes principales de acción. Esto porque los escasos sistemas de gestión tecnológica existentes contrastan visiblemente con las inversiones millonarias que regularmente eroga la Federación en las instituciones de educación, y demás organismos gubernamentales, para la adquisición de licencias de software de aplicación para sus equipos y tecnologías de cómputo.

Por otra parte, la gestión de la seguridad informática es difícil y compleja de implementar, no importando el tamaño de la institución, por lo que se requiere diseñar una política que involucre los fines reales de la institución, y que considere además los entornos socio-económicos y políticos, aunado al hecho de que exista una motivación y sustento para llevarla a cabo. En este contexto, esta investigación surge de la necesidad de analizar la manera en la que se podrían eficientar los recursos fiscales que manejan los organismos públicos y que involucran directamente a sus recursos humanos, su infraestructura y los mecanismos legales asignados a dichas entidades para el desempeño de sus funciones sustantivas y en las cuales el aspecto informático juega un papel cada vez más relevante.

En el caso de instituciones como el IPN se debe buscar una evolución organizacional en las áreas nuevas o en dónde la dinámica propia de la especialidad sugiere un ritmo diferente al burocrático. La mejora continua de su tecnología y de los servicios que ofrecen obliga a coordinar los esfuerzos de las diferentes áreas organizativas del IPN involucradas en asegurar el entorno informático de la institución. En un principio se

[1]Ver la nota "México, entre los 5 países con mayor seguridad informática," en la URL: http://noticias.universia.net.mx/ciencia-nn- tt/noticia/2009/06/03/15331/mexico-5-paises-seguridad-informatica.html [recuperada el 20 de mayo de 2011]

desarrollaron manuales técnicos que resultaron inviables para ser implementados en áreas administrativas por la falta de conocimiento técnico especializado por parte de los cuadros encargados de aplicarlo; además de que muchos procedimientos generalmente se basaban en manuales de procedimiento desarrollados con argumentos más administrativos que técnicos.

En la actualidad, las políticas para la gestión de los riesgos informáticos en el IPN están plasmadas en la ley orgánica del instituto y su reglamento interno, los cuales fijan las reglas, controles y procedimientos para estandarizar la forma en que el instituto previene, protege y mitiga los riesgos de seguridad en las distintas instancias de operación.[2] Sin embargo, para una correcta implementación de mecanismos de gestión del riesgo informático en el IPN se requieren cambios organizacionales que acepten, e incluso agilicen, la adopción de elementos enfocados a la prevención de los riesgos informáticos.

De acuerdo con los modelos tradicionales de gestión de la tecnología (véase, por ejemplo, Palop y Vicente, 1999; Hidalgo et al., 2002), los procesos básicos de captación, análisis, difusión y reestructuración corporativa son entendidos desde sus distintas concreciones en función de las necesidades y cultura del entorno de la organización misma. Para tal efecto es imprescindible poder traducir las necesidades de los usuarios a fin de poder planificar y direccionar la información obtenida a favor del entendimiento de la interacción organizacional con el mismo. Estas ideas serán reflejadas en información y datos que nutrirán la inteligencia tecnológica en la toma de decisiones que permita una gestión de los riesgos informáticos para difundir los mecanismos de protección más ampliamente. Los programas de inteligencia competitiva deberán cubrir 4 áreas, a saber (Rodríguez, 1998:77):

a) Seguimiento de las tecnologías
b) Evaluación y pronóstico de tecnologías
c) Evaluación de competidores, vendedores, proveedores y colaboradores.
d) Seguimiento y análisis de tendencias de mercado, sociales, reguladoras con

[2] LEY ORGANICA DEL IPN.- Articulo 4 : numeral viii, ix, xiii, xv, xvii.
Gaceta Politecnica.31 de julio 2006 reglamento para la administración, operación y uso de la red institucional de cómputo y telecomunicaciones del IPN.

impacto en las actividades científicas y tecnológicas.

Para el IPN la innovación incipiente en la seguridad informática se nutre también de la gestión dinámica de la información, así como de las áreas externas (proveedores, distribuidores, colaboradores, clientes). Así, la inteligencia competitiva aplicada al campo de la seguridad informática debería reflejarse en la implementación de un programa sistemático para identificar, recolectar y analizar información sobre el entorno y las actividades propias de los usuarios de su red de cómputo, así como para hacer uso oportuno de tal información para la toma de decisiones, especialmente en relación con la aparición de nuevos virus y amenazas cibernéticas. Las aplicaciones específicas de la Inteligencia tecnológica se centran en 5 grupos:

a) Estrategia tecnológica y del negocio
b) La adquisición de tecnologías
c) La gestión del portafolio de proyectos
d) La asignación de recursos de ciencia y tecnología
e) Las operaciones de producción

El objetivo de este esquema de inteligencia sería reforzar la competitividad de la Dirección de Cómputo y Comunicaciones del IPN (DCYC) para que tenga forma de obtener las respuestas oportunas y racionales a las señales que ofrece el entorno en materia de riesgos informáticos. Sin embargo, tal y como lo señalan Solleiro y Castañon (2008), el potencial del concepto de inteligencia tecnológica se diluye frecuentemente porque se le utiliza como sinónimo de la aplicación de herramientas estandarizadas, las cuales tienden a estar basadas únicamente en datos duros, sin que se haga un análisis más profundo de los factores actuantes.

De esta forma, la organización de la inteligencia tecnológica resulta una asignatura pendiente para instituciones como el IPN que se han visto empujadas a adaptarse a los retos derivados por la crisis económica y la exigencia por la asignación eficiente de los recursos públicos.

Como lo señala Ortega (2010), la problemática particular del área de la seguridad de la

información institucional requiere de un estudio para poder gestionar de forma efectiva sus elementos tecnológicos y poder sugerir la implementación de cambios eficientes en la estructura organizacional. Aunque la mayor parte de la literatura existente sobre la gestión de recursos se ha enfocado a la administración de los medios disponibles para alcanzar fines específicos, aún falta la discusión de un enfoque complementario de sistemas de gestión informática que analice la problemática desde el punto de vista del usuario, de la autoridad y de los administradores de las TIC, con el fin de evitar ver a la seguridad informática como una carga administrativa, sino como un método para incrementar la eficiencia operativa del IPN.

Debido a que la seguridad informática es un tema que normalmente no representa una prioridad administrativa para el IPN, esta investigación se guía por las siguientes preguntas de investigación:

1) ¿Cuál es el desarrollo de los SGSI en el entorno mundial?

2) ¿Cuál ha sido el desarrollo de la gestión del cambio tecnológico en la Seguridad Informática en la DCYC?

3) ¿Qué pautas son susceptibles a desarrollar o implantar para tener un SGSI en la DCYC?

Con base en lo anterior, el presente trabajo de investigación plantea la realización de un diagnostico sobre la gestión del cambio tecnológico aplicado a la seguridad informática y propone acciones en los ámbitos estructurales, de gestión de la información y transferencia tecnológica. El caso de estudio que se plantea es el de la Dirección de Cómputo y Comunicaciones (DCYC) del IPN.

Figura 1: Entrada Dirección de Cómputo y Comunicaciones del IPN

Se partirá de la descripción del entorno institucional y su relación con los cambios tecnológicos en el área de la computación. Este cambio está vinculado con la gestión de la seguridad informática. Esta tesis se basa en la experiencia profesional que el autor tuvo dentro de la DCYC, y propondrá acciones que fortalezcan la mejora continua en la gestión de la seguridad informática del IPN.

Es importante señalar que la intención del trabajo, no es solamente realizar una revisión crítica de la actual gestión que realiza el personal de la DCYC, sino también abordar el potencial de la gestión tecnológica para el buen funcionamiento de la DCYC a través de

una revisión de sus técnicas, herramientas y prácticas organizacionales, planteando una batería de propuestas para su desarrollo. Aunque el estudio se centra en la DCYC, los procesos básicos de captación, análisis, difusión y resultados organizacionales son recogidos desde sus distintas facetas en función de las necesidades y cultura del IPN. Por lo que se prestará atención a los problemas más recurrentes que experimenta la institución en el terreno de la seguridad informática.

El Instituto recibe un presupuesto anual de 6800 millones de pesos en 2010 y en 2011 manejo 10900 millones casi un aumento de 60%. Con estos recursos se atiende las 40 ECU´s en su infraestructura, personal y crecimiento. Se debe destacar que existen aproximadamente 40000 nodos de datos fijos, además de los equipos portátiles y móviles cuyo registro es difícil de obtener pero que sin duda son incluidos en las políticas de seguridad informática del IPN.[3]

[3] Revisar: http://www.dipotados.gob.mx/LeyesBiblio/pdf/PEF_2011.pdf
http://www.josefina.mx/noticia.php?noticia=954

CAPÍTULO 1: LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

1.1 Calidad en Actividades del Sector de las TIC

Es común escuchar que cuando las personas hablan de la era de la información, hablen de disfrutar de las facilidades del e-mail, las redes sociales, la información en línea, videos, música, cómputo en la nube y demás servicios informáticos que anteriormente significaban un costo excesivo y pocas oportunidades de poder tener acceso a ellos de manera institucional, aunque fuera de manera restringida. Ahora podemos utilizar estos servicios a través de distintos proveedores y por diferentes medios de distribución, con precios accesibles y en la mayor parte del territorio nacional, lo que ha creado, en general, mejores condiciones de vida para la población (OCDE, 2009).

Machlup (1962) acuño la frase "sociedad de la Información", utilizando términos como producción y distribución del conocimiento, el cual fue entendido como un activo intangible para nuevas fuentes de trabajo y riqueza que ya no estarían ligadas al esfuerzo físico, ni siquiera a la presencia material o a un sitio determinado de trabajo.

Sin embargo, la concepción actual de lo que se entiende por Sociedad de la Información está influida por la obra del sociólogo japonés Masuda (1981), quien introdujo nuevos términos de análisis que tienen relación con las posibilidades de poder realizar casi cualquier actividad social, laboral y económica a través de medios tecnológicos, puesto que son la tecnología y la innovación quienes ahora pueden dirigir las tendencias de crecimiento del mercado mediante algoritmos que permiten predecir preferencias de la sociedad en cuanto a hábitos de compras de bienes y servicios; creando así expectativas comerciales y de mercado mediante la publicidad mediante la homogeneización de la conducta social.

Esta revolución del análisis de la información por personas o grupos, cuya finalidad es monopolizar mercados estandarizando productos y servicios ha provocado en los gobiernos y las instituciones, la protección del que hoy en día es uno de los activos más valiosos: los datos ya codificados y almacenados. Anderson (1980) es el primero en utilizar el concepto de seguridad informática. En un informe que solicitó el gobierno de

EE.UU., Anderson describe conceptos que desde entonces se han vuelto cotidianos, términos tales como “Amenaza” en el sentido de un intento deliberado y no autorizado de: a) Acceder a la información; b)Manipular información; y c)Convertir un sistema en no confiable o inutilizable. Todos los cuales permanecen vigentes.

Estos escenarios tan actuales han sido tratados en todos estos años como posibilidades a la hora de identificar riesgos en la exposición accidental o impredecible de la información en las instituciones, o cuando hablamos de una violación en la integridad de las operaciones debido al mal funcionamiento del hardware, arquitectura incompleta o incorrecto trabajo del software. Mediante este análisis de posibilidades se puede detectar las vulnerabilidades de un sistema informático, esto es fallas conocidas, ya sea en el hardware o en el diseño del software, o la operación de un sistema administrativo que se compromete al exponer la información de una forma incorrecta.

El enfoque actual es en cómo ha evolucionado la sociedad en su conjunto, y parte importante de este desarrollo lo es el comercio electrónico, la automatización de procesos remotos, las estimaciones de producción en consecuencia existe una nueva organización del trabajo al estilo indicado por Adam Smith (1999).

Algunos especialistas en las áreas de TIC se han agrupado como hackers y gurús de los sistemas de comunicación e informática que a través de foros exponen vulnerabilidades de los mismos y que son contratados por las empresas para proteger o evaluar el nivel de seguridad informática en ellas (Picouto et al., 2007).

Las empresas e instituciones están invirtiendo grandes recursos en la adquisición de tecnología y especialistas con el objetivo de proteger sus sistemas y la información que por ellos se mueve, la especialización de los productos o procesos que la institución desarrolla a partir de sus actividades sustantivas, el grupo de clientes a los que sirve y las tecnologías utilizadas para ello (Abell, 1980).

Los activos de la organización, entre los cuales la información es uno muy valioso, pueden perderse durante un ataque informático, ya sea interno o externo, porque se realiza de forma silenciosa y repercute en las relaciones personales, la efectividad del trabajo, la imagen de la empresa, la confiabilidad de las transacciones y en la reputación

a cada nivel de la organización. Por lo mismo muchas instituciones tratan de protegerse invirtiendo recursos, tanto en hardware como en recursos humanos, para poder brindar mayor certeza y confiabilidad a los usuarios del servicio que prestan; pero estas soluciones son tan variadas, tanto en precios y tecnología como a nivel de tamaño de empresas, que la seguridad de la información se convierte en un laberinto que puede llevar a las organizaciones a un callejón sin salida.

Así, el primer interés de las instituciones es proteger su información de los ataques más comunes, y/o de los virus más peligrosos; para ello un programa antivirus efectivo es casi una obligación dentro de las organizaciones que no quieren dejar la puerta abierta a los intrusos así que los sistemas de Firewall e IPS se incorporan a este modelo de arquitectura de seguridad; pero aún así los recursos humanos más eficientes y el hardware más actualizado no garantizan el éxito en la batalla, si al mismo tiempo no se presenta la interacción e integración entre el capital humano y el organizacional. Esto para que un plan de innovación y gestión del conocimiento pueda ser exitoso. Sí no se tiene contemplado un Plan Estratégico, es decir un sistema de gestión de la seguridad alineado a la estrategia tecnológica de la organización, es muy probable que el sistema se colapse a la hora de un ataque informático.

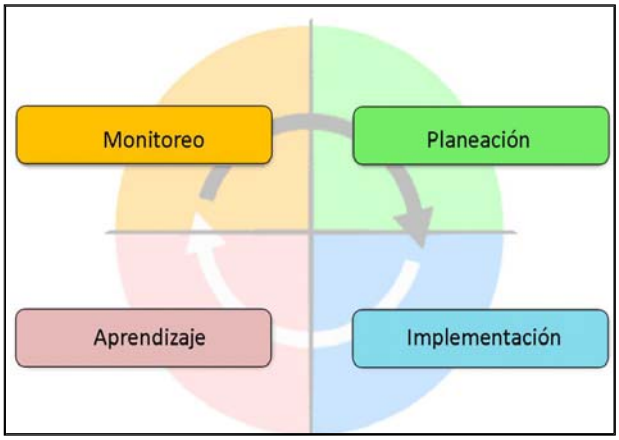
1.2 Naturaleza de un Sistema de Gestión de Seguridad Informática

El modelo que se ha tomado como guía en esta tesis parte de la implantación, operación, monitoreo, mantenimiento y mejora en cualquier clase de organización. En particular, el diseño y la implementación de un Sistema de Gestión de Seguridad Informática (SGSI) están influenciados directamente por las necesidades, los objetivos, el tamaño, los empleados, los procesos y la estructura organizacional. Por consiguiente, un SGSI tiende a ser único en todos los aspectos. Este tipo de modelos está alineado con las guías y principios recomendados por la OCDE en materia de seguridad informática (Alexander, 2007:22).

La figura siguiente presenta un esquema basado en la norma ISO 27001:2005 que a su vez se apoya en el círculo virtuoso de Deming, de cómo debe realizarse una dinámica

organizacional centrada en fomentar cambios en los procesos que realiza la gestión de la tecnología en todos los ámbitos.

Figura 2. Modelo del ciclo virtuoso de Deming



Fuente: Modelo basado en la norma ISO 27001:2005.

La fase de planificación establece el alcance del modelo para una institución, identificando y tasando los activos para posteriormente realizar un análisis y evaluación del riesgo que ayude a determinar que riesgos son aceptados o transferidos.

En la fase de implementación, según el ciclo de Deming, se llevan a cabo las acciones que deben implementarse para el control o mitigación de los riesgos seleccionados.

El monitoreo es una parte esencial en ella se deben de tener establecidos las rutinas y procedimientos con métricas que permitan evaluar el desempeño del SGSI.

En la fase final del ciclo, llamada aprendizaje o mejora continua, se toman las decisiones pertinentes para reaccionar ante incidentes y tomar también acciones preventivas. La idea es llevar a la excelencia el SGSI, por lo tanto este modelo es compartido por los estándares ISO 9000:2000 e ISO 14000:2004.

Basado en el modelo anterior, esta tesis se enfoca en privilegiar el papel del capital humano, que es uno de los activos más valiosos, junto con la infraestructura y los datos ya codificados de una organización en el terreno informático, mediante una adecuada gestión de la tecnología. En esta perspectiva, la tesis propondrá un mecanismo para revisar el proceso de diseño organizacional del departamento de informática desde una

perspectiva cognitiva, que le permita a la comunidad politécnica recibir los beneficios de las nuevas tecnologías sin exponerse a los virus, troyanos, gusanos y demás programas maliciosos que se dispersan en Internet, sin olvidar que el principal objetivo del IPN es fomentar el conocimiento. Dada estas condicionantes, es pertinente señalar, como lo hacen Nonaka y Takeuchi (1999), que esta cualidad exige que una organización como el IPN realice esfuerzos para innovar constantemente en un intento por hacerle frente a lo inesperado, es decir, hacer esfuerzos por desarrollar el conocimiento competitivo.

Por esta razón se aborda aquí el cambio tecnológico desde la estructura organizacional, pasando por la infraestructura, su grado de madurez y la transferencia tecnológica de la Seguridad informática en el IPN tomando en cuenta el tamaño que tiene la organización, su acervo de capital humano y las herramientas tecnológicas disponibles para ello.

Como en todo sistema de gestión de seguridad de la información primero debemos identificar los activos de información que se poseen para conocer su impacto en la institución. De tal importancia es la metodología a seguir que existen varias normas y referencias de buenas prácticas para evaluar el nivel de seguridad informática. En ellas se apoyan gobiernos y empresas. Entre las más difundidas están la Information Technology Infrastructure Library (ITIL) (APM Group, 2008), creada en el Reino Unido por la Agencia Central de Computo y Telecomunicaciones (CCTA), y la (OGC) Oficina Gobernativa de Comercio.

La ITIL provee un marco de referencia adaptable a las organizaciones para asegurar las mejores prácticas en calidad de servicio y como superar las dificultades asociadas con el crecimiento de los sistemas. Es la base para poder estructurar un sistema que pueda tener métricas de control, que es el siguiente paso y para ello nos apoyaremos en COBIT (Control Objetives for Information and related Technology). Esta tecnología de seguridad informática es el marco aceptado de buenas prácticas para el control de TI y el riesgo que conllevan. Su fortaleza estriba en poder implantar el Gobierno de las TI y mejorar los controles de TI. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez.

Idealmente las empresas e instituciones buscarían estar certificadas en ISO 27001, porque

define su enfoque organizacional como la aplicación de un sistema de procesos junto con la identificación e interacciones de estos procesos y su gestión.

En el caso del IPN existe una normatividad publicada en la gaceta politécnica en el año 2006 en donde se plasma la necesidad de modernizar la tecnología, la transparencia, fomentar la eficiencia y racionalidad confiriendo a la coordinación de servicios informáticos. El control de la operación, uso y administración corresponde a la DCyC que a su vez dirige el Subcomité de programas de cómputo y sistemas de información encargado de motivar la generación de políticas y la gestión con relación a la seguridad de la información que busca regular las condiciones de operación del sistema y dicta los lineamientos en el tema de la seguridad informática. Sin embargo, dentro de sus funciones no contempla el evento de que ocurran intrusiones en el sistema, haciendo falta una política específica de seguridad de la información[4]. Cuando la información se ha perdido, modificado o robado es posible que falten los procedimientos de control y registro de estas actividades. No obstante, el departamento de seguridad informática no tiene la capacidad jurídica, ni el personal suficiente para dar seguimiento a estos actos de intrusión, que afectan diariamente las actividades sustantivas del IPN y que van en detrimento de la imagen que se ha forjado el instituto a lo largo de su historia como pionero del cómputo en México.

Asimismo, llama la atención que el tema de la seguridad informática no se haya generado una reacción académica dentro de la institución, ya que los planes y programas de estudio de las diferentes ingenierías y licenciaturas afines al tema no incluyen tópicos de seguridad enfocados a una especialización en el tema; siendo la excepción ESIME Culhuacán, donde existe una Maestría de Seguridad Informática (MISTI) aprobada en 2009 que se enfoca a la encriptación de señales5. En la parte administrativa resulta casi increíble que el trabajo administrativo no tenga ninguna capacitación en cultura de seguridad informática, lo que obliga al personal a trabajar sin siquiera aplicar las reglas básicas de seguridad en equipos de escritorio (*password*) para el inicio de sesión.

[4]Un ejemplo de ello ocurrió el pasado 15 de septiembre de 2011, véase la página http://www.bsecure.com.mx/featured/mexico-ha-sobrevivido-ataques-ddos-por-parte-de-anonymous-y-ahora/

[5] Para mayores datos véase la página de la maestría en la URL: http://www.posgrados.esimecu.ipn.mx/

No obstante, en 2006, se realizó un esfuerzo por delimitar alcances y responsabilidades en la red institucional al publicarse el reglamento para la operación, administración y uso de la Red Institucional de Cómputo y Telecomunicaciones del IPN (Gaceta Politécnica, 2006). Este documento es de suma importancia ya que en él se designan las entidades responsables del uso, operación y administración de la red institucional de telecomunicaciones y cómputo, en ella también se identifica a los actores de su regulación y sus alcances.

Este reglamento es el único documento institucional que se refiere a la administración y algunos tópicos de seguridad inherentes a los procesos de comunicación y cómputo. Describe los servicios a los cuales tiene derecho el personal docente y de apoyo, así como, los alumnos y ex alumnos.

El documento menciona que son las unidades de informática (UDIs) las encargadas de implantar y vigilar las políticas de seguridad, además de las políticas y lineamientos emitidos por la Coordinación. También se describe un Comité Institucional de Tecnologías de la información y las Comunicaciones que consta de tres subcomités. El encargado de vigilar y proponer la seguridad del equipo de cómputo y la red institucional El Subcomité de Programas de Cómputo y Sistemas de Información.

Mientras la inversión en seguridad informática se incrementa alrededor del mundo, en el IPN todavía no figura como un componente del Plan Estratégico Organizacional; incluso naciones tan pequeñas como Estonia ya han publicado su estrategia de cyberseguridad[6] (MODE, 2008). En dicho documento se manifiesta la necesidad de una cultura de seguridad informática motivada por los gobiernos ante las amenazas que afectan a todos los niveles de la sociedad.

Así, se busca reducir las vulnerabilidades en forma conjunta entre el gobierno, empresas y la cooperación internacional. La estrategia del gobierno de Estonia se basa en cuatro políticas de seguridad:

1) Aplicación de un sistema de gradual de seguridad informática.

[6] El Congreso Mexicano ha definido concepto de ciberseguridad. Véase la pagina del DOF en la URL: http://www.dof.gob.mx/nota_detalle.php?codigo=5208001&fecha=06/0972011

2) Incrementar la cultura de la seguridad informática.

3) Desarrollo de un marco legal que asegure y garantice la operatividad de sistemas de información.

4) Promover la cooperación internacional en seguridad informática.

Estos elementos se pueden adoptar en el IPN para fomentar una cultura de seguridad Informática, la cual se convertiría en una estrategia apropiada para sentar la diferencia entre prestar un servicio de transferencia tecnológica o persistir en la existencia de un problema.

Recapitulando, la mención de las anteriores normas y mejores prácticas tiene como fin exponer que en la literatura existen planteamientos exitosos, por lo que el objetivo de esta tesis no es crear un nuevo método sino el de identificar los existentes y aplicarlos con la finalidad de sentar las bases para un proceso de mejora continua en el caso de la DCYC.

1.3 La Naturaleza de un Sistema Informático y la Gestión del Cambio Tecnológico

Para conocer la importancia que las TIC tienen dentro de la planeación estratégica de una organización se tiene que tener un conocimiento de los conceptos principales de forma homogénea. Por ejemplo, el hardware es uno de los elementos más conocidos de un sistema informático, y corresponde a todo aquello que tiene forma física en el sistema informático. En términos generales, el hardware consiste de diferentes elementos mecánicos, magnéticos, ópticos, eléctricos y electrónicos que forman parte del sistema. La función de ellos es la de servir de interface de entrada/salida en el manejo y almacenamiento de la información. Estos elementos interactúan entre sí por medio de un bus o circuito impreso que los conecta con la unidad de procesamiento (CPU) que se encuentra en la computadora y que junto con el microprocesador le brinda al sistema su capacidad de cálculo.

Los dispositivos de entrada permiten ingresar datos, comandos y programas para que interactúen con el CPU. Dentro de los ejemplos más comunes de dispositivos de entrada se encuentra el teclado, convirtiendo las pulsaciones sobre él en impulsos eléctricos que

serán codificados y se convertirán en datos y al ser codificados serán la información con la que interactúa el humano y la máquina.

En versiones más modernas tenemos el Touch Screen, el cual funciona básicamente de la misma manera solo que los impulsos eléctricos son generados al presionar una membrana en la que se encuentra codificada una matriz de posicionamiento que genera datos binarios, y que puede interpretar la computadora, el lector de código de barras, utiliza un programa que interpreta la posición de ese código logrando proporcionar gran información en poco tiempo y ahorrando el mismo en tareas repetitivas o de inventario, los dispositivos biométricos necesitan de un programa de gran complejidad capaz de identificar por métodos térmicos, geométricos y químicos la identidad de un individuo. Dispositivos más comunes pero indispensables para ingresar datos son el mouse y el lápiz óptico para aplicaciones específicas.

Los dispositivos de salida, como la pantalla, que es el dispositivo visual estándar de salida, sirven para observar los datos que serán ingresados y muchas veces también es donde observamos el resultado del procesamiento. Para efectos de resultados gráficos es necesario contar con una pantalla con buena resolución que se obtienen por la densidad de puntos por pulgada llamados pixeles. Entre más pixeles soporte el dispositivo mejor será su resolución. Esta información es procesada en una tarjeta de video que se encuentra embebida en la tarjeta madre del CPU ó que puede estar en un slot de escalamiento. La calidad de información grafica que nos presente depende directamente de estos elementos. Otro dispositivo de salida muy común es la impresora. Pueden ser de impresión de caracteres, impresoras de línea ó matriz, impresoras de inyección de tinta, impresoras térmicas y la más especializada es la impresión laser, capaz de imprimir hojas completas a gran velocidad y calidad.

Los dispositivos de almacenamiento son auxiliares en el procesamiento de los datos ingresados al CPU en la llamada memoria RAM (Memoria de Acceso Aleatorio), la que tiene la particularidad de almacenar los datos mientras tenga alimentación eléctrica. Existen dispositivos especializados por medios magnéticos que son capaces de almacenar información sin depender de la corriente eléctrica y se encuentran conectados al CPU por

medio de buses de datos conocidos como memoria ROM (Memoria de solo lectura) y coloquialmente como HD (disco duro). También existen otros dispositivos de almacenamiento óptico como el CD-ROM y el DVD que se valen de un lector/grabador óptico para poder acceder a la información y para grabar nueva información en los dispositivos.

En los últimos años se ha desarrollado un tipo de tecnología llamada memoria Flash, o coloquialmente memoria USB, que es independiente de las conexiones eléctricas tradicionales y cuyo funcionamiento se basa en una interfaz electrónica, pero no en campos magnéticos u ópticos, y ha revolucionado la portabilidad de la información. La comunicación se realiza a través de un puerto serie en la máquina, en donde se conecta al sistema informático para guardar la información que contiene.

El software es todo aquel método que se utiliza para el tratamiento de la información. Es un componente intangible, lógico del sistema informático. El estudio del software nos lleva al estudio de los lenguajes de programación para las computadoras y los procesadores en específico. Esta programación tiene diferentes orientaciones y existen programas para dar instrucciones al procesador, los programas de utilidades y aplicaciones y los sistemas operativos, entre otros.

El software tiene dos vertientes para su estudio: los de sistema operativo (software del sistema), los cuales funcionan de interface entre la computadora y el usuario interpretando comandos, controlando las interrupciones lógicas para la interacción del hardware, controla la asignación de memoria, mantenimientos de archivos en disco duro, etc.; y el software de aplicación, el cual se utiliza para administrar las distintas tareas que puede desarrollar una computadora desde un procesador de textos, bases de datos y hasta una simulación de moléculas. Existe un tratamiento particular para el sistema operativo de red y el software de programación.

Tabla 1: Características del Sistema Operativo

1)	Lograr el mejor rendimiento de los recursos (Hardware)
2)	Ejecutar las aplicaciones y resolver los problemas inherentes a él
3)	Realizar trabajos multitarea, administrando las diferentes aplicaciones y Garantizando recursos para cada una de ellas
4)	Interpretación de comandos
5)	Administración de dispositivos entrada/salida
6)	Manejo de errores y tolerancia a fallos
7)	Protección; resguardando los programas y aplicaciones de un usuario respectode otro que utilice la misma computadora, pero en diferente perfil
8)	Multiacceso o acceso remoto
9)	Habilidad para evolucionar en la integración de hardware y aplicaciones novedosas
10)	Manejar las comunicaciones de red

Fuente: Elaboración propia

Un sistema informático, como conjunto, está formado por hardware, software y el capital humano. Los sistemas informáticos tienen la capacidad de unirse y formar un sistema mayor a través de la interconexión. Los diseñadores de sistemas utilizan ciertas reglas llamadas protocolos para poder realizar la interconexión entre diferentes sistemas informáticos y potenciar sus capacidades. En un principio era necesario que estos sistemas estuvieran físicamente cerca. En la actualidad pueden estar en cualquier sitio del mundo que tenga conectividad en internet y se puede lograr integrar n número de sistemas informáticos para igual número de aplicaciones y capacidades de procesamiento.

Los sistemas informáticos fueron en el origen las herramientas que revolucionaron las actividades de las empresas e instituciones, la revolución de la sociedad de información se le atribuye a la PC y el desarrollo de sistemas mayores que permitió integrar grupos interdisciplinarios con nuevas expectativas y visiones en la innovación y creación del conocimiento.

Con base en la exposición anterior podemos determinar que la interacción entre el dispositivo electrónico y el individuo es impulsado por la creación y difusión del

conocimiento. Encontramos los modelos de innovación lineales conocidos como:

Technology push, modelo de innovación que utiliza la ciencia básica y el diseño de ingeniería para ofrecer soluciones al mercado y puede o no tener una aceptación comercial.

Market pull, modelo de innovación que busca satisfacer necesidades del mercado basados en el desarrollo de productos que ya tiene un mercado cautivo.

En ambos escenarios existe la necesidad de una gestión que permita la transferencia tecnológica, pues de otra forma se corre el riesgo de que en lugar de realizar una acción preventiva y planificada se caiga en lo que comúnmente suelen hacer la instituciones frente a la seguridad informática: actuar de formare activa (Alexander, 2007:13)

CAPITULO 2: LAS COMUNICACIONES COMO HERRAMIENTA DE DESARROLLO

2.1 Presentación

En la actualidad la importancia que están cobrando los sistemas de comunicaciones se refleja en aplicaciones tales como las redes de investigadores, las redes sociales, las redes de ayuda, etc. Gracias a estos avances tecnológicos ahora pueden interactuar no solo desde las instituciones educativas sino desde prácticamente cualquier sitio, lo que ha dado nacimiento a las TIC.

Las TIC son un conjunto de servicios, redes, software y equipo que tienen como finalidad mejorar la calidad de vida de las personas integrando sistemas de información propios y complementarios. Las TIC tienen la ventaja de poder contener imagen, voz y datos; por separado, o en conjunto, como lo son los tradicionales medios como la radio, la televisión y las páginas web estáticas. La digitalización del contenido de cualquiera de estos medios puede ser almacenada, procesada y sintetizada bajo demanda del cliente o del usuario.

La comunión entre las computadoras y el internet ha modificado la sociedad desde los años noventa del siglo pasado aunque su desarrollo tecnológico es independiente, aún se debe elegir correctamente el tipo de herramientas, soportes y canales para el tratamiento, la forma, el registro, almacenamiento y difusión de contenidos.

Las innovaciones en este campo son vastas pues existen tecnologías como la pizarra digital, los blogs, las redes sociales, los podcast y la web 2, que se utilizan en todo tipo de aplicaciones como pueden ser las educativas, las sociales, las informativas y otras tantas que con base en el planteamiento de la ingeniería social pueden no ser bien intencionadas, ejemplos como portales falsos de banca en línea, descarga de software antivirus, música, premios e invitaciones apócrifas a eventos son las aplicaciones que más innovaciones tienen, para atraer visitantes y seguidores que dependiendo de su capacidad y conocimiento son sus futuras víctimas.

En resumen, las ventajas para los usuarios del uso de las TIC son:

- La gran difusión de la información contenida
- La velocidad de difusión

- Desarrollo e intercambio de ideas entre diferentes actores a través de redes de apoyo o listas de discusión
- Permitir el aprendizaje interactivo y la educación a distancia
- Nuevas formas de desempeñar el trabajo presencial
- Difusión del conocimiento e información para modificar la estructura social

Sus desventajas:

- Sociedades comunicadas pero indiferentes.
- Consumismo de equipos de computo y comunicaciones.
- Obsolescencia prematura de tecnologías.
- Aumento en el costo de la tecnología.
- Falta de privacidad.
- Aislamiento
- Pereza física
- Fraude
- Merma en los puestos de trabajo

La interacción de estas tecnologías no puede existir sin organizaciones que vigilen y administren los contenidos, los recursos, las tendencias tecnológicas y la identidad de las organizaciones que utilizan estos medios.

Los sistemas de comunicaciones se basan principalmente en la conmutación de circuitos y paquetes. En la conmutación el emisor y receptor se comunican entre sí utilizando de forma permanente el circuito intermedio, al igual que se hace en una llamada telefónica. En la conmutación de paquetes la comunicación se realiza en tramos de datos que llevan la información al destino utilizando los sistemas intermedios solo mientras se transmite. Internet se basa en este último sistema.

2.2 La Internet

El origen de internet data de 1962 cuando la empresa de I+D Bolt Beranek & Newman de EE.UU. propone una red global; esta idea es llevada a ARPA (Advanced Research

Projects Agency) donde en 1960, Paul Baran publica un trabajo con fines militares sobre una red segura de comunicaciones capaz de sobrevivir a un ataque nuclear, la innovación sería dividir el mensaje original en múltiples fragmentos, se enviaría mediante diversas rutas posibles para luego armarlo una vez llegado a su destino, esta idea fue reforzada con una teoría sobre colas aplicada a las redes de comunicaciones publicada en 1964 por Leonard Kleinrock (Anderson, 1980).

No obstante, estos estudios sobre los sistemas de conmutación de circuitos no satisfacían a los investigadores porque perdían capacidad de cómputo teniendo que gestionar líneas telefónicas. Por lo que nuevamente la innovación tuvo que asistir a la ciencia utilizando solo un computador para gestionar las comunicaciones y separando el resto de las computadoras por su naturaleza. El impulsor de esta idea fue Wesley A. Clark y en 1969 surge ARPANET con solo 4 computadoras conectadas, comenzando así su crecimiento exponencial. Para 1973 aparece el primer programa de correo electrónico. En 1983 cambia al actual protocolo de comunicación de paquetes conocido como TCP/IP, los progresivos avances en la conexión entre empresas y redes tanto públicas como privadas integran la actual Internet (Kogut, 2003).

Una vez que el sistema de comunicación conecta los sistemas informáticos de diferentes tamaños surgen las aplicaciones que transforman la sociedad en su conjunto, los protocolos de SMTP (Correo Electrónico), FTP (Transferencia de archivos de cualquier tamaño) y el lenguaje de programación HTML, que fue creado por Tim Berners, dio lugar a navegadores como Netscape y al subsecuente boom de Internet y sus múltiples servicios (Tilman, 2003).

Lo que en un principio solo buscaba conectar el mayor número de computadoras, al final se convirtió en una enorme masa de interconexiones, razón por la cual surgieron diferentes organizaciones para guiar el desarrollo y mantener la organización de la red, tales como Internet Engineering Task Force (IETF). La parte técnica es regulada por Internet Society, que es responsable de la actual organización de Internet, la cual se detalla en el estándar RFC 1602, siendo sus prioridades el crecimiento y la evolución de Internet.

El Internet Engineering Task Force es el principal cuerpo encargado del desarrollo de las nuevas especificaciones de los estándares de Internet. La IETF está conformada por grupos de trabajos individuales, agrupados a su vez en áreas. Cada una de las cuales es coordinada a su vez por uno o más directores de área.

Internet Architecture Board es un asesor consultivo técnico de la Internet Society. Es un comité de vigilancia del resto de las organizaciones que se han mencionado. Confirma el nombramiento de cargos y revisa los protocolos y procedimientos usados por Internet. Además regula la asignación de direcciones de IANA y la administración de los RFC. Su funcionamiento esta descrito en el estándar RFC 2850 (COBIT, 2008), como se menciona más adelante.

Como se ha descrito el conjunto de tecnologías que permiten la adquisición, producción almacenamiento, tratamiento, comunicación, registro y presentación de información, en forma de voz, imágenes, texto en señales de distintas naturalezas como lo son acústica, óptica ò multimedia por medio de innovaciones en electrónica, informática y comunicaciones, todas ellas lo hacen de forma particular y son las organizaciones las que por medio de la gestión modifican los prototipos para que pueden interactuar con sistemas anteriores y sus funcionalidades pueden ser explotadas por la mayoría de la sociedad.

Una de las características que permite el desarrollo de las TICs, es que por sí misma permite que la información esté disponible para casi cualquier individuo en cualquier latitud del planeta, la digitalización de la información la convierte en intangible pero con un potencial de difusión impresionante, por medio de las redes de comunicación que transmiten de forma transparente la información no importando lo lejos en distancia de origen y consulta de los datos.

La velocidad y disponibilidad de la información genera una percepción diferente sobre ésta dada la posibilidad de cambiar en un instante todo el contexto del usuario. Para explicar esta situación se han buscado términos como ciberespacio o autopistas de información. La idea es entender que las comunidades con temas afines pueden trabajar de manera continua, aumentado los resultados de las investigaciones de forma ilimitada.

Las comunidades virtuales han llevado a las TIC un paso más allá en su evolución mediante las tecnologías de web 2 que se alejan de los grupos de espectadores recibiendo solo información e integrando aplicaciones multimedia que permiten el debate en tiempo real, tanto entre individuos, como entre grupos de individuos; transformando a los cibernautas en sujetos activos que modifican el entorno según sus intereses.

Sin embargo, el anonimato que proporciona la cibersociedad, junto con la posibilidad de estar presente de manera virtual en casi cualquier sitio y horario también es explotado por algunos individuos faltos de ética, quienes se dedican a entorpecer la difusión del conocimiento, ya sea mediante la modificación de la información, o mediante la generación de información negativa o errónea, o a falsificar o suplantar identidades, sin dejar a un lado el gran negocio que esto representa generando ganancias millonarias en piratería, corrupción y lavado de dinero, por lo que en el mundo digital solo una gestión adecuada de la seguridad informática puede mantener a salvo a los usuarios de las organizaciones que administración dicha información, sin embargo ni la delincuencia está a salvo de las vulnerabilidades de las TIC.[7]

2.3 Instituciones Reguladoras de Internet

Una vez expuesta la forma en que se dan las comunicaciones así como su importancia en el desarrollo es necesario señalar las asociaciones que se encargan de su regulación a nivel mundial, particularmente las que están más relacionadas con internet, por tratarse del sistema que engloba la tendencia de *cloud computing*. A continuación se describen las principales asociaciones.

La Internet Assigned Numbers Authority (IANA) tiene desde 1990 la función de asignar direcciones IP globales, así como la administración de los servidores DNS raíz y cualquier otra asignación necesaria de un protocolo de Internet. Sin embargo en 1998 pasó a formar parte de la estructura técnica de Internet Corporation for Assigned Names and Numbers (ICANN). Cabe señalar que IANA conserva sus funciones respecto a IETF como se especifica en el RFC 2860 (COBIT, 2008).

[7] Revisar http:\\www.proceso.com.mx/?p=287269 Anonymous vs zetas:la otra guerra.

El World Wide Web Consortium es un consorcio internacional que produce estándares para la red mundial (World Wide Web). El producto de su trabajo es una recomendación, equivalente a estándares en la red. Algunos ejemplos de ello son el protocolo HTTP o las hojas de estilo en cascada (CSS).

El Computer Emergency Response Team tiene su origen en el Instituto de ingeniería de software de la Universidad de Carnegie Mellon en Estados Unidos. Fue creado en 1988 después del primer gusano creado por el ingeniero T. Morris. Su objetivo es responder rápidamente cuando ocurre un incidente de seguridad.

Como se puede entender de la descripción de las actividades de estas asociaciones, la influencia de la gestión del internet realizada por ellas es el resultado de la apertura al cambio tecnológico y las nuevas aplicaciones en la red. A continuación se describe el diseño de esta red.

2.4 La Arquitectura en las Comunicaciones

Todo equipo en la red se identifica por una dirección IP única compuesta de 32 bits en el llamado estándar IPv4. Gracias a la aparición de NAT (Network Address Translation) por la escases de direcciones IPv4. Ahora podemos encontrar redes corporativas representadas en Internet por solo una IP. Las primeras organizaciones identificaron sus servidores por IP públicas también conocidas como homologadas en Internet que reconocían al servidor específico y a su propietario en todo el mundo. En el futuro inmediato se tendrá que hacer uso de la nueva arquitectura de distribución de direcciones IP en su versión 6, lo que implicará un cambio en la administración de las organizaciones.

Para que la información entre sistemas informáticos viaje entre origen y destino es necesario que los sistemas de manejo de datos sepan qué hacer con los paquetes que generan y reciben de manera que puedan gestionar una aplicación de destino en el interior de la computadora o la dirección de un servidor en la red interna o externa que proporciona un servicio específico.

En las redes de los sistemas informáticos existen dispositivos denominados *routers* que permiten distinguir entre el tráfico interno y aquel cuyo destino es una red externa. De su correcta configuración depende la capacidad de conexión de unas computadoras con otras. La arquitectura de comunicaciones que se lleva a cabo en el *backbone* de Internet es susceptible, sin embargo, de cambios debido al rápido avance de las tecnologías electrónicas en comunicación.

La escasez de direcciones IP junto con la implementación de NAT en los *routers* públicos han dado lugar a la aparición de multitud de redes. Las computadoras que se encuentran en estas redes no tienen una IP pública de Internet sino que dependen para su conexión a Internet de la IP del *router*. La arquitectura de Internet se basa en *backbones* o redes troncales. Estas redes son propiedad de universidades, gobiernos o empresas. El acceso a estas redes troncales se lleva a cabo a través de Proveedores de Acceso a Internet (ISP). Los ISP suelen conectarse con otros proveedores de áreas geográficas cada vez mayores, los cuales se conectan finalmente a una de las redes troncales que señalamos. Existen puntos de Intercambio de Internet (IXP) donde todos los ISP se conectan entre sí, cuando estos puntos de intercambio no son propiedad de uno de los proveedores ISP que intercambian se les llama Puntos neutros de internet (NAP).

Este intercambio se realiza a través de un protocolo que permite redefinir las rutas dinámicamente y que se denomina Border Gateway Protocol (BGP), que se encarga de dirigir la enorme cantidad de paquetes que se transmite en los IXP y en las redes troncales. Este protocolo tiene su origen en el llamado "Gateway Protocol" que se utilizó en los primeros tiempos del Internet.

Como se mencionó antes, los sistemas informáticos se comunican entre sí por medio de una dirección IP. Sin embargo en cada uno de ellos, los distintos protocolos de aplicación, como el servicio de SSH, se distinguen por el número de puerto de conexión. Históricamente los diferentes números de puerto de han asociado a la aplicación de forma que se les conoce como puertos conocidos o servicios conocidos.

Los puertos se definen en paquetes de 16 bits, en un rango de 0 a 65,535. Éstos se dividen, a su vez, según el protocolo de transmisión en TCP/UDP. Los 1024 primeros

bits del (0 al 1023) son administrados por la IANA. El resto se consideran libres para que los usen la comunidad de usuarios. El cuadro siguiente proporciona algunos ejemplos de estos dispositivos:

Tabla 2: Tipos de Protocolos de Transmisión

20/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros)–datos
21/tcp	FTP File Transfer Protocol (Protocolo de Transferencia de Ficheros)–control
22/tcp	SSH, SCP, SFTP
23/tcp	Telnet comunicaciones de texto inseguras

Fuente: Elaboración propia

La comunicación entre las computadoras se lleva a cabo entre direcciones IP, sin embargo para el ser humano no es fácil acordarse de esta serie de números, por lo que usualmente se le asigna un nombre significativo. En el conjunto de Internet se ha definido un sistema coordinado que permite registrar los nombres de las direcciones IP, que en este modelo se llaman dominios y que se asignan a partir de servicios de registro, normalmente pagando por este servicio. Los dominios de alto nivel son denominaciones acuñadas que se asignan a redes geográficas como .mx para México, funcionales como .edu para instituciones educativas o genéricas como .com para negocios.

El funcionamiento es a través de un archivo llamado hosts que se encuentra en el sistema operativo. En este tipo de archivo se define un nombre de dominio y su traducción a numero IP de forma que siempre que se utilice este nombre para identificar una máquina. La computadora buscará primero la traducción en ese archivo. Sin embargo, no es necesario tener en un archivo todos los nombres de dominio del mundo, para ello existe un servidor DNS que se encarga de resolver todos los nombres y hacer la traducción necesaria para cada computadora. El protocolo DNS nació en 1983 con los estándares RFC 882 y 883 y actualmente está normalizado por los estándares RFC 1034 y 1035. Los servidores DNS públicos son administrados por la IANA y en él se encuentran todas la IP registradas por dominios (COBIT, 2008).

CAPITULO 3: BASES DE LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA EN LA ESTRUCTURA ORGANIZACIONAL

El análisis de la gestión de la seguridad informática, como tema de esta tesis, se relaciona con tres aspectos: la estructura organizacional, la tecnología y el individuo; por lo que se atenderán primeramente las bases de una estructura organizacional como el principal elemento de análisis en el proceso de gestión de la seguridad informática.

De acuerdo con la teoría de las organizaciones, la variable tamaño determina el tipo de estructura organizacional a emplearse y su naturaleza dictará que tanto se puede utilizar el resultado de la especialización de sus empleados. El tamaño de las grandes organizaciones encuentra un ciclo virtuoso al poder contratar un mayor número de empleados operativos con la subsecuente ventaja económica sobre la competencia resultado de la especialización (Robbins, 1987: 103).

Por otra parte, las organizaciones educativas tienden a ser encasilladas en términos de organizaciones burocráticas donde la diferenciación es horizontal debido a su gran tamaño (generalmente mayor a los 2,000 empleados). De acuerdo con Robbins (1987: 113), una estructura organizacional tiende, en el mejor de los casos, a ser permanente pues tiende a ser altamente incongruente con la dinámica que obedece a la generación de conocimiento básico, investigación y transferencia tecnológica a la sociedad.

En este trabajo se busca establecer una diferenciación en la gestión de la seguridad informática que, siendo vertical, sirva para tener la capacidad de coordinar las unidades de especialización horizontal que resultaran de la expansión espacial en la estructura organizacional de la institución, ya que una institución de gran tamaño puede llegar a ser manejada como una pequeña empresa con poco estimulo a la innovación, conflictos de administración y el cambio de cultura organizacional (Robbins, 1987:118).

Este aumento en el tamaño de la estructura es necesario dada la evolución del

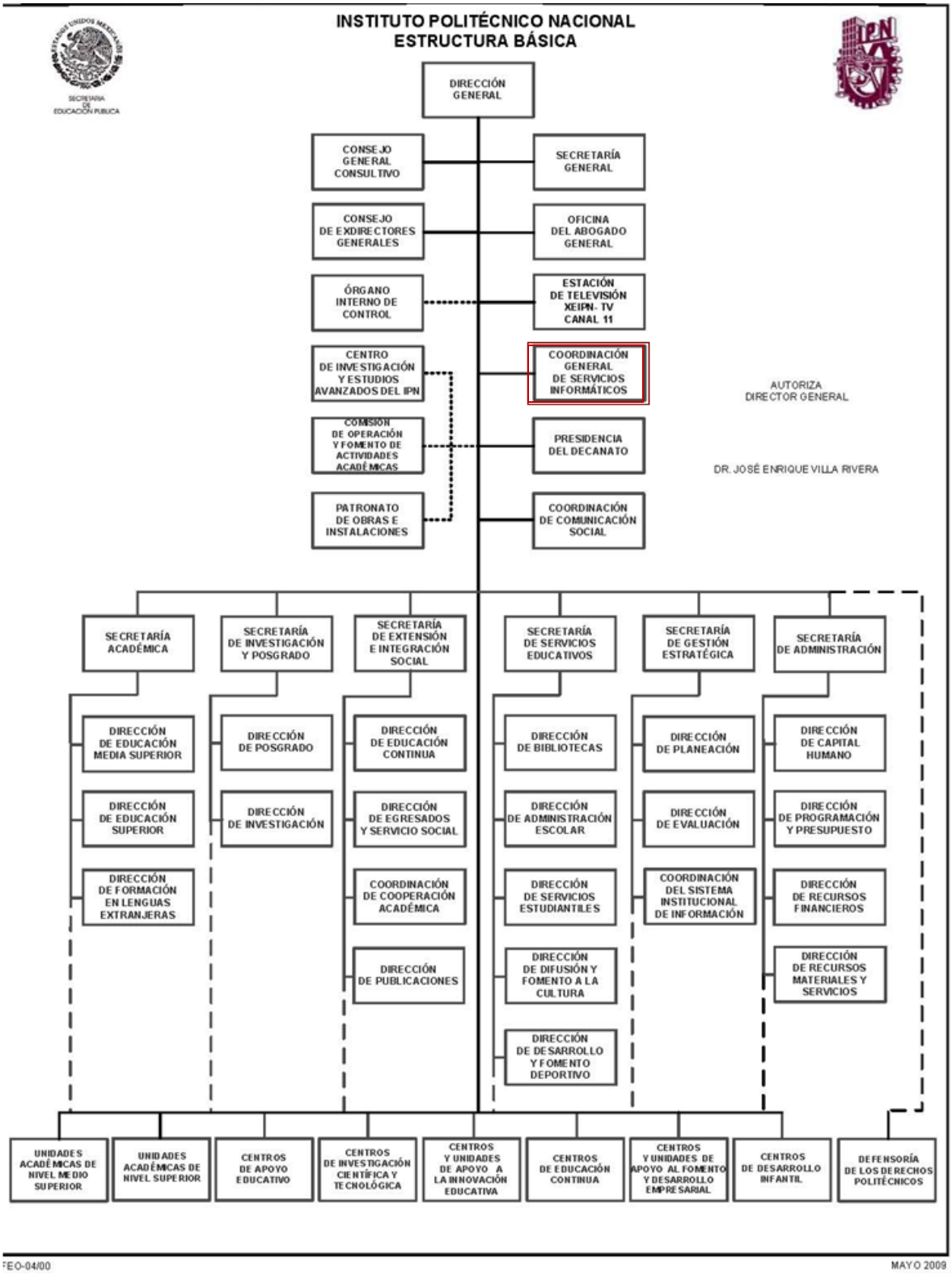
proyecto y que sin duda hasta el momento las buenas prácticas de seguridad informática están latentes en toda actividad que se desarrolle entre individuos. Entonces, definiremos el tamaño de la organización de acuerdo al número de empleados; y de forma inherente podemos definir el tamaño organizacional mezclando la cantidad de empleados con su nivel de eficiencia.

Es importante aclarar que no es fácil argumentar si una organización realiza actividades semejantes con 30 empleados o con 130; pues en ambos casos los mismos 30 empleados pueden ser igualmente eficientes. De esta forma se puede decir que las relaciones humanas son subjetivas y en ellas se encuentran inmersas cantidad de información relativa a procedimientos y diferencias de especialidad. Aun así, la cantidad de empleados en una organización nos habla de la capacidad de absorción de trabajo "per se". La evidencia de las organizaciones de servicios de gobierno nos indica que la diferenciación horizontal se desarrolla principalmente en organizaciones más grandes.

3.1 Estructura Organizacional

Los diferentes ámbitos en donde se desarrollan las instituciones de educación hacen necesaria una estructura organizacional como herramienta para la división de las diferentes actividades del trabajo, la clasificación de una actividad compleja en unidades, a fin de que los individuos sean responsables de un conjunto limitado de actividades y no de la actividad como un todo que lleven al logro de los objetivos institucionales (Mintzberg, 1988). Esta división del trabajo viene acompañada de las jerarquías necesarias para una correcta división y supervisión de las actividades asignadas al personal operativo. La supervisión persigue la mejora continua mediante la identificación y simplificación de funciones. Es decir, las organizaciones estables tienden a ser sometidas a un proceso de innovación continua (Weick, 1982).

Figura 3: Estructura Organizacional IPN



Fuente: Dirección de Planeación IPN

En el caso del IPN se reconoce la importancia de las estructuras organizacionales para el logro de los objetivos generales, sin embargo en ellas existen interrelaciones individuales, es decir, interacción social de individuos con un propósito particular y aunque las actividades están orientadas a cumplir metas especificas estas son influenciadas por acciones internas. Desde la observación institucional las actividades están estructuradas y los individuos conscientes de que su trabajo está bien desarrollado con el apoyo de herramientas tecnológicas y la organización, alcanzando con ello las metas trazadas de una forma eficiente.

3.2 Elementos de la Estructura Organizacional

La estructura de una organización sirve para indicar cuáles son las tareas y la responsabilidad de cada uno de los miembros, así como los efectos de sus acciones en los resultados de la organización, de tal forma que se minimicen las imprecisiones y contradicciones en las tareas encomendadas; obteniendo un sistema de comunicación y de toma de decisiones estructurado (Robbins, 1987).

Uno de los principales elementos que contribuyen a una mejor administración de la estructura organizacional es la división del trabajo. Desde un punto de vista estratégico tendremos que mencionar a la jerarquización de las funciones de la Institución en un orden de rango, grado o importancia. En una segunda etapa dividiremos las funciones en departamentos que agrupen las actividades en unidades definidas por la similitud de las actividades. Las ventajas de la simplicidad de funciones y actividades para los operarios permiten que en un futuro las tareas puedan ser automatizadas aumentando su efectividad.

Definiendo efectividad como el logro de objetivos es posible entender la relación de los resultados obtenidos y aquellos que se habían previsto alcanzar. Para Robbins, hacer las cosas de forma correcta, obteniendo un alto grado de cumplimiento de los objetivos planificados es el signo de una organización eficiente (Robbins, 1987).

Entendiendo la eficiencia en el uso de los recursos como la relación entre los

recursos utilizados y los programados. Entonces una organización debe hacer las cosas correctas, obteniendo un alto grado de aprovechamiento de los recursos transformándolos en productos o servicios.

Finalmente, deduciendo como coordinación la sincronización de los recursos y esfuerzos que componen el entorno de trabajo organizacional, es posible analizar las metas como el lograr los objetivos de manera rápida, oportuna, en armonía y unidad.

En este sentido describiremos las estructuras organizacionales más representativas.

3.3 Estructuras Organizacionales Funcionales

La estructura de tipo funcional es la más utilizada por las instituciones o empresas que tienen servicios específicos. Utilizan con eficiencia los recursos especializados, facilitando la supervisión de actividades ya que los encargados de las líneas de servicios solo deben ser expertos de una gama limitada de prácticas y es posible identificar donde hace falta la especialización de habilidades. A continuación se mencionarán algunas ventajas de este tipo estructura:

Las funciones sustantivas de los responsables son fácilmente identificadas. El dominio en las tareas desarrolladas brinda la oportunidad de automatizar y desarrollar una especialización en el personal. La generación de grupos de capital humano dinámicos, derivado de las particulares formas de solucionar los problemas de los diferentes individuos involucrados en la estructura funcional correspondiente porque reduce la duplicación de infraestructura.

Por otra parte, la identificación de necesidades de personal, infraestructura y de nuevos productos o servicios son actividades organizacionales aceptadas y comprendidas. Además, los responsables jerárquicos conocen las condiciones locales, generando circuitos de comunicación estables.

A su vez, la descentralización de las decisiones en los cargos especializados tiene algunas desventajas, tales como: las personas que trabajan sobre esta estructura

están más enfocadas a desarrollar su trabajo que el servicio o producto que se presta o se vende, provocando una baja optimización organizacional. La identificación de los circuitos de comunicación informales entre distintas áreas es compleja, afectando la coordinación entre ellas. Se crean interdependencias de escala de trabajo; por lo que debido a la alta especialización existe una pérdida de autoridad de mando.

La existencia de una subordinación múltiple provoca problemas en la delimitación de responsabilidades. Existe una tendencia de competencia entre unidades y especialistas haciendo prevalecer el enfoque y el punto de vista particular. También existe una tendencia a la tensión y conflictos en la organización derivada de la pérdida de visión de objetivos comunes, esta diversidad de objetivos particulares crea divergencias y conflictos entre los especialistas. Finalmente existe una generación de contactos improductivos, la subordinación múltiple impide la comunicación de problemas entre unidades provocando confusión operativa y desorientación en cuanto a cómo alcanzar los objetivos.

3.4 Estructura Lineal

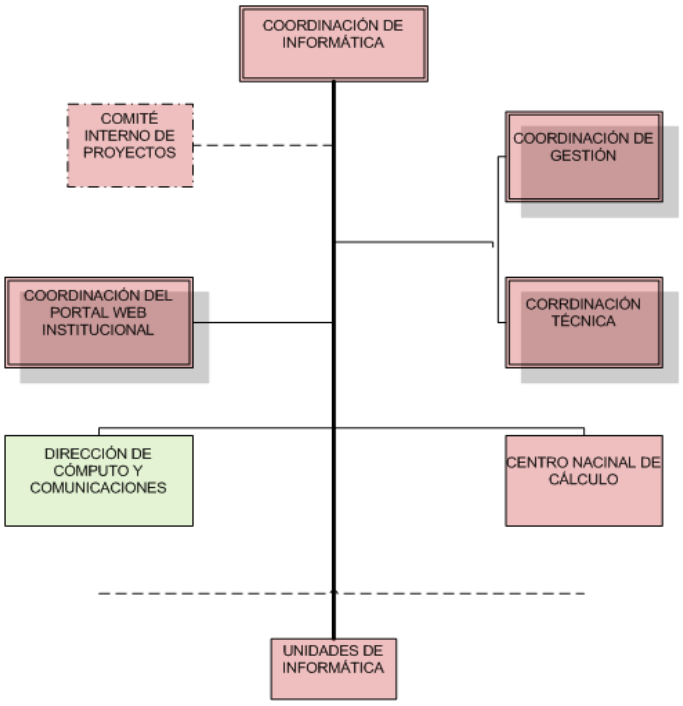
La división del trabajo se agiliza debido a su forma, donde es fácil de identificar las líneas de autoridad y de establecer líneas de comunicación más claramente, permitiendo un acercamiento deseable entre la autoridad y los subordinados. La dificultad de poder manejar este tipo de estructura se observa cuando se intenta establecer una división de trabajo horizontal porque está enfocada a personal con un alto grado de especialización. De acuerdo con Michael Porter (1987), la estrategia horizontal coordina las metas y estrategias de las unidades de negocios relacionadas. Comúnmente la alta dirección es absorbida por la operación ya que la organización depende de sus decisiones y del control que tenga de los subordinados, dejando de lado la planeación, la investigación y la innovación.

3.5 Organización Linea-Staff

La combinación de la organización lineal y la formal pretende sumar los beneficios de una línea ágil de mando y la eficacia y cumplimiento de objetivos comunes establecidos por la línea formal.

Las actividades fundamentales de la organización están fuertemente ligadas a los objetivos, las actividades intermedias, las metas correspondientes a órganos complementarios representan actividades cotidianas. En el caso de que los objetivos de la organización cambien, la estructura línea-staff también se ajustará. Es decir los órganos de la línea de mando están pensados para cumplir los objetivos del exterior de la organización mientras que la estructura de staff está ocupada en cumplir las metas de los demás órganos ya sean del personal o de la línea de dirección.

Figura 4: Estructura Organizacional CGSI.



Fuente: Dirección de Planeación IPN.

Las características principales de la organización línea-staff radican en la fácil identificación de la principal autoridad, la que coincide con una sola línea formal

de mando. La existencia del órgano staff carente de autoridad de línea pero con la función de prestar servicios autorizados y asesoría a todos los órganos de la institución tiene la formalidad en la expresión de las recomendaciones, pero solo eso. Para que esas ideas sean ejecutadas necesitan del apoyo de la línea directa de comunicación, por lo que la comunión entre los niveles superiores y subordinados se establece. El staff o grupo especializado aconseja al jefe de línea de mando sobre algunas de sus actividades. El aseguramiento de la disciplina y el mando se logra por la jerarquía, en cambio el grupo de especialistas provee ideas.

Lo deseable de este tipo de organización, y por lo cual se propone analizarla para el caso de la DCYC del IPN, es el valor que se pone en el capital humano operativo altamente especializado, brindando una asesoría experta, buscando la innovación en las actividades cotidianas; principalmente se busca la coordinación entre los órganos de línea y los órganos de staff en forma conjunta.

En resumen podemos observar que el tamaño de la organización está ligado a su estructura organizacional; es decir, el cambio tecnológico es más fácil de absorber al tener una estructura que crece en forma horizontal en la cual se contratan especialistas que contribuyen a la adquisición de capacidades tecnológicas, convirtiéndose en una ventaja frente a la estructuras organizacionales de la competencia. Esta especialización está acompañada invariablemente de una gran diversificación de especialidades y decisiones similares al resolver problemas equivalentes lo que implica que existe un alto grado de estandarización.

Por otra parte, la estructura vertical presenta rasgos muy característicos: es muy marcada en su estructura jerárquica, tiende al aumento de la documentación, de la estandarización y de la extensión horizontal; sin embargo tiene características que no son tan deseables como son el incremento en la descentralización de la toma de decisiones, lo que debilita la jerarquía creando cotos de poder (Thompson, 1959: 17).

Estos cotos de poder nacen de la relaciones humanas entendiendo la complejidad de ellas, sustituyendo la complejidad técnica por la burocracia y en este sentido se

puede determinar que las relaciones de trabajo son únicas dada la diversidad de escenarios físicos, limitaciones de presupuesto, diferencias en el tamaño del staff y las regulaciones propias de la estructura.

No se debe dejar de lado la importancia dentro de la estructura vertical que dadas las condiciones de descentralización de esta estructura será eficiente dentro de las grandes instituciones sí los mandos altos tienen una visión profesional de su trabajo y no particularizan o trasladan el trabajo a relaciones personales generando interacciones desgastantes y estadísticamente significativas. El problema es que este traslado de relaciones, o "cacicazgo," va en contra de la delegación de la toma de decisiones, ya que un gerente "dominador" no está dispuesto a dividir su poder personal y control sobre las actividades de la institución (Gerwin, 1979: 71). Por tanto, el tamaño determina la estructura, pero la estructura no es la causa del tamaño (Robbins, 1987: 108). Lo que también implica que la diferenciación vertical aumenta el tamaño de la institución debido a la alta especialización horizontal.

Estos efectos indeseables de la estructura organizacional son mitigados por la formalización de la autoridad en la estructura, esto se logra mediante la sanción a la violación de las reglas escritas, de los procedimientos y de las relaciones laborales. Sin embargo estos vicios de la organización dependen en gran medida de la ética laboral de los administradores a todo nivel, ya que la formalidad cuando es enfrentada a las relaciones personales se vuelve muy débil (Robbins, 1987:111), mientras que la formalización termina siendo validada por una vigilancia directa o por una regulación formal. Las implicaciones de una vigilancia directa son el aumento en el tamaño de las rutinas en la organización porque cualquier nueva reglamentación afecta la operación de las comunicaciones, aunque ésta se puede hacer eficiente a través de la tecnología, con lo que se puede tener un control más estrecho de la cantidad y calidad del trabajo, aunado a que la mejora continua derivada de la calidad permite innovar sobre los procedimientos mediante un cambio de las reglas internas y de los manuales de operación; haciendo posible la predicción de resultados con la calidad deseada. Este incremento en la

formalización de la autoridad también contribuye a la descentralización y aumenta la efectividad de las instituciones.

3.6 La Estructura Organizacional y la Tecnología

Ahora se discutirá la relación entre la estructura organizacional y la tecnología, la cual, además de persistente, es compleja porque son interdependientes. En la teoría organizacional el tema de la tecnología se refiere a la información, equipamiento, técnicas y procesos que ayudan a transformar los insumos en productos o servicios (Robbins, 1987:125). Para todas las actividades organizacionales, el hecho de que aumenten los flujos de trabajo y las operaciones técnicas debido a un incremento en la complejidad tecnológica y/o de un aumento de la automatización en las actividades termina por afectar de manera directa el funcionamiento y el tamaño de la estructura organizacional.

La existencia de estas interacciones ha llevado al desarrollo de tres enfoques teóricos principales, los cuales se presentan en el siguiente cuadro:

Tabla 3: Tipología de Woodward

Tipo de Producción	**Descripción**	**EJEMPLO**
Producción Unitaria	Producción de elementos o unidades únicas que tiene procesos pequeños	ARTESANOS
Producción en Masa	Producción masiva de elementos mediante producciones en serie	MANUFACTURA
Producción de Procesos	Producción continúa de elementos por procesos con un grado de complejidad	PETROQUÍMICA

Fuente: Elaboración propia basado en Woodward (1980)

Joan Woodward (1980) plantea que las organizaciones se adaptan a la tecnología existente en ellas, que el tamaño de la producción está ligado al incremento de los niveles de complejidad y sofisticación tecnológica y las diferentes medidas que se

pueden identificar son: Niveles jerárquicos, estructura de control, los componentes administrativos, el grado de formalización y como se lleva a cabo esta. Woodward propone una clasificación preliminar de las instituciones, dado que pueden estar abajo del promedio, en el promedio o por arriba del promedio en términos del éxito económico o efectividad organizacional, dependiendo de la categoría tecnológica según Woodward. El cuadro siguiente presenta la tipología propuesta por esta autora para identificar los tipos de producción que se presentan en una organización.

En esta división se pueden apreciar las distintas relaciones entre la tecnología y la estructura organizacional de la empresa, por lo que su efectividad será el resultado del ajuste entre ambas categorías. Por otra parte, el grado de diferenciación vertical aumenta con la complejidad tecnológica, y podemos observar que los componentes administrativos varían directamente con el tipo de tecnología; lo que significa que cuando la complejidad tecnológica aumenta, también lo hace, de forma proporcional, la administración y el personal calificado. Este incremento de la estructura organizacional se percibe cuando se presenta una transición de la producción en masa hacia la producción de procesos, con lo que también aumenta la complejidad, aunque la formalidad tiende a decrecer, al igual que el alcance del control en las organizaciones. Estos cambios se pueden ver en el siguiente cuadro.

Tabla 4: Efectos de Cambios en los Tipos de Producción

Estructura	Producción Unitaria	Producción en Masa	Producción por Procesos
Niveles Verticales	3	4	6
Alcance de Control	24	48	14
Relación Gerentes/Empleados	1:23	1:16	1:8
Especialización	Alta	Baja	Alta
Complejidad	Baja	Alta	Baja
Formalización	Baja	Alta	Baja
Centralización	Baja	Alta	Baja

Fuente: Elaboración propia basado en Woodward (1980)

En este cuadro se observa que la producción en masa es la que tiene la línea de autoridad (centralización) más elevada, la formalización más alta en actividades una baja proporción de trabajadores especialistas, debido a gran división del trabajo, un mayor número de supervisores controlando las actividades de producción y la mayor complejidad de la producción.

Otro enfoque organizacional es proporcionado por Charles Perrow (1991), quien aborda la forma en que la tecnología se utiliza en diferentes procesos de las empresas, observando que existe dos tipos de situaciones: 1) Variedad de tareas, debido a que hay excepciones en el trabajo cotidiano, las cuales pueden ser inesperadas, porque a veces ocurren eventos extraordinarios en la conversión de procesos; y 2) Problemática Analizable, que es cuando las actividades del trabajo y sus problemas encuentran una solución bajo el análisis. Estos problemas analizables pueden ser resueltos con procedimientos y estandarizaciones técnicas conocidas. Los problemas no analizables son resueltos por la experiencia, la intuición o la sabiduría.

Para Perrow existen cuatro tipos de tecnología, a saber:

1) Tecnologías rutinarias: Tienen pocas excepciones y los problemas son fáciles de analizar;

2) Tecnologías de Ingeniería: Tienen un gran número de excepciones, pero puede ser manejado de una forma racional y sistemática;

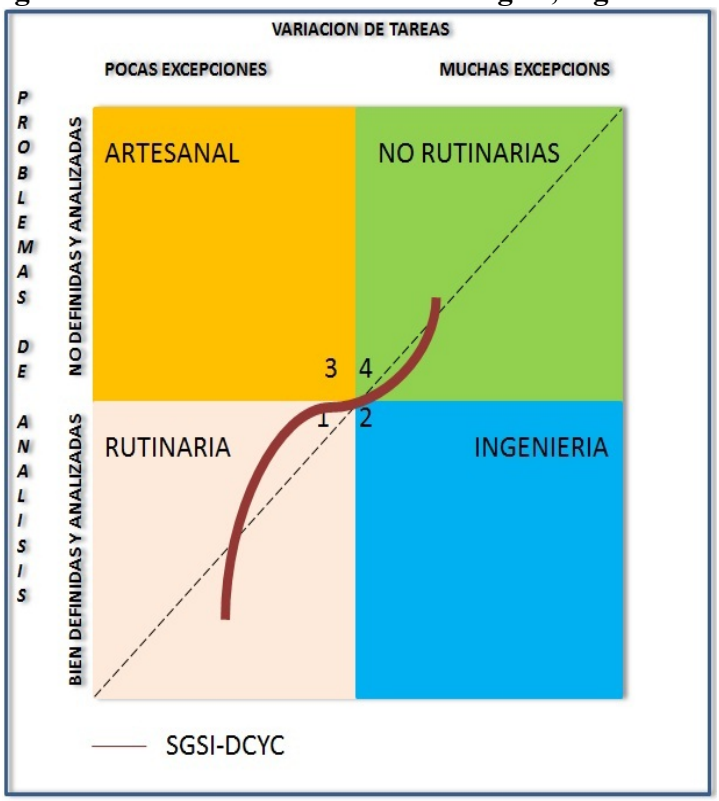
3) Tecnologías artesanales: Sabiduría de la experiencia para resolver problemas relativamente difíciles pero con un conjunto limitado de excepciones; y

4) Tecnologías No rutinarias: son caracterizadas por muchas excepciones y dificultad para analizar el problema.

En resumen, de los cuatro casos mostrados, el estudio sistemático de problemas, usando la lógica y el análisis racional, se realiza en las tecnologías 1 y 2; mientras que los problemas que se presentan tienden a ser solucionados mediante la

intuición, las conjeturas y la experiencia, pero sin algún tipo de análisis, corresponden a las tecnologías 3 y 4.

Figura 5: Clasificación de las Tecnologías, según Perrow



Fuente: Elaboración propia basada en Perrow (1991), y en las tareas desarrolladas en el SGSI-DCYC.

Perrow logra identificar cuatro elementos clave que son modificados por la tecnología: La cantidad de discreción que es utilizado para completar tareas. El poder de grupos de control en áreas exitosas y estratégicas. La medida de interdependencia entre estos grupos, y la medida en que estos grupos participan en coordinación de su trabajo, utilizando comentarios o planeación de otros.

Lo que quiere decir que las tecnologías rutinarias se deben controlar con la estandarización y supervisión, lo que implica un alto grado de centralización y formalización. Por otro lado las tecnologías no rutinarias demandan flexibilidad, descentralización de la toma de decisiones y un alto grado en la interacción de los miembros, además se caracterizan por tener un mínimo grado de formalización.

Las tecnologías artesanales resuelven sus problemas haciendo uso de gran conocimiento y experiencia, lo que implica descentralización. Finalmente, las tecnologías de ingeniería tienen muchas excepciones pero pueden ser analizadas en los procesos identificados en la figura anterior. De acuerdo con Robbins, estas tecnologías pueden tener decisiones centralizadas pero son flexibles en la formalización de actividades (Robbins, 1987:132).

Se puede concluir que las organizaciones tienen diversos tipos de tecnología, que en la mayoría de las rutinas de trabajo las decisiones comúnmente se hacen de forma centralizada y con alto grado de formalización y finalmente que las organizaciones tienden a tener mayor número de rutinas estandarizadas, mayor formalización y centralización y un mínimo de tecnologías no rutinarias.

Finalmente, James Thompson: (1959) nos muestra la medida en que los departamentos de una organización son interdependientes con los recursos y materiales necesarios para realizar sus actividades. Para este autor, la baja interdependencia quiere decir que un departamento es capaz de hacer su trabajo con una baja intensidad de interacción, consulta o intercambio de materiales. Por el contrario una alta interdependencia significa que el departamento tiene un constante intercambio de recursos.

Para Thompson existen cinco tipos de interdependencias, a saber:

1) Interdependencia reunida (*pooled interdependency*) es cuando existe una baja interdependencia entre los departamento. De esta forma el trabajo no fluye entre las unidades. La contribución de cada unidad es para el bien común de la organización, pero el trabajo es independiente.

2) Interdependencia de vinculación larga (*long-linked*), se presenta si las tareas a desarrollar son secuencialmente interdependientes, lo que hace que entren en esta categoría. Esta tipología se caracteriza por tener una secuencia fija de pasos repetitivos y requiere de altos niveles de coordinación entre las tareas para llegar a ser eficientes, la forma de lograrlo es la planeación y la integración vertical.

3) Interdependencia secuencial (*sequencial interdependence*), se refiere a que las

salidas de un departamento son las entradas de otro en forma serial. Esto representa un alto nivel de interdependencia, en consecuencia se crea una alta necesidad de mecanismos de integración horizontal.

4) Tecnología mediadora (*mediating technology*), es la que provee productos y servicios a través de clientes o mediadores externos y al hacerlo permite que cada departamento trabaje independientemente. Para lograr la coordinación se depende de que la tecnología pueda generar medidas tanto de categorización como de estandarización. Las organizaciones con este tipo de tecnologías son moderadamente flexibles en la entrega de productos y servicios, existiendo incertidumbre ante una gran demanda. El uso de las salidas de diferentes unidades integradas por categorías, estándares y procedimientos reduce el costo de largos vínculos que requieren planeación a través de demasiadas tareas para garantizar el adecuado flujo de trabajo.

5) Tecnología Intensiva (*intensive technology*), es la respuesta personalizada a un conjunto diverso de contingencias. La respuesta depende de la naturaleza de los problemas y de su variedad, los cuales no pueden dictaminarse con antelación. La naturaleza de la solución de problemas mediante esta tecnología requiere de un alto nivel de gestión, los diferentes departamentos involucrados tienen una gran interdependencia por lo que se estila una gran integración horizontal y constante ajuste, además de que la supervisión es entre los gerentes es personal asegurando un mutuo ajuste.

Con la finalidad de tener una visión más general de estas tipologías, el cuadro siguiente presenta una comparación entre los efectos de las tecnologías en la organización que fueron mencionadas antes:

Tabla 5: Comparación de las Tipologías de Tecnologías Organizacionales

Autor	Rutinaria	No-Rutinaria
Woodward	Masiva, Proceso	Unitaria
Perrow	Rutinaria, Ingeniería	Artesanal, No-rutinaria
Thompson	De vinculación Larga/Mediadora	Intensiva

Fuente: Elaboración propia basado en los autores mencionados.

CAPÍTULO 4: GESTIÓN ACTUAL DEL SISTEMA DE SEGURIDAD INFORMÁTICA EN EL IPN: EL CASO DE LA DCYC

En este capítulo se discutirá la gestión de la seguridad informática en el Instituto Politécnico Nacional tomando como punto de referencia el caso de la Dirección de Cómputo y Comunicaciones (DCYC), la cual es el área responsable de las actividades informáticas en el Instituto. El enfoque de este capítulo es descriptivo y tomará en consideración los aspectos teóricos discutidos en los capítulos anteriores para revisar la situación operativa y funcional de la DCYC.

La DCYC es un área de la administración central del IPN dependiente de la Coordinación General de Servicios Informáticos. De acuerdo con su página web[8], es la responsable de administrar y controlar la infraestructura y los servicios institucionales de cómputo y comunicaciones impulsando la incorporación y utilización de las TIC con criterios de consolidación, optimización, ampliación de la cobertura, fortalecimiento y modernización, así como de mejora continua en la atención a la comunidad politécnica usuaria de estos servicios, en la productividad de su personal y como un elemento sustancial en la toma de decisiones.

La evolución de la DCYC se puede entender mediante el análisis de los cambios que ha experimentado a lo largo de su historia, los cuales han sido moldeados, a su vez, por los avances científicos y tecnológicos en el campo de las telecomunicaciones. Los antecedentes de la DCYC se remontan a la creación del Centro Nacional de Cálculo en 1964, del Centro de Investigación y Desarrollo de Tecnología Digital en 1984, del Centro Nacional de Información y Documentación Tecnológica en 1986 y del Centro de Investigación Tecnológica en Computación en 1987, así como de la Dirección de Informática en 1982, que fue suprimida en 1985 como consecuencia de la política de racionalización de las estructuras emitida por el Gobierno Federal,[9] reubicando sus funciones en la Dirección de Evaluación y en el Centro Nacional de Cálculo.

[8] http://www.dcyc.ipn.mx/WPS/WCM/CONNECT/DCYC/IPN/INICIO/INDEX.HTM
[9] http://www.decanato.ipn.mx/pdf/tomo3.pdf:79

Sin embargo, a finales de 1989 cobró fuerza la conformación de una red de cómputo, que dio pié al establecimiento del Programa Académico de Cómputo, orientado a apoyar y fortalecer los procesos educativos, de investigación y de actualización de su comunidad académica. En 1993, se inauguró el Edificio de la Central Inteligente de Cómputo y se instauró el Programa Institucional de Cómputo y Comunicaciones como el medio para integrar y dar congruencia a todas las acciones tendientes a ofrecer tecnologías avanzadas dentro de este campo y con el objeto de optimizar todos los aspectos del quehacer académico y administrativo del Instituto.

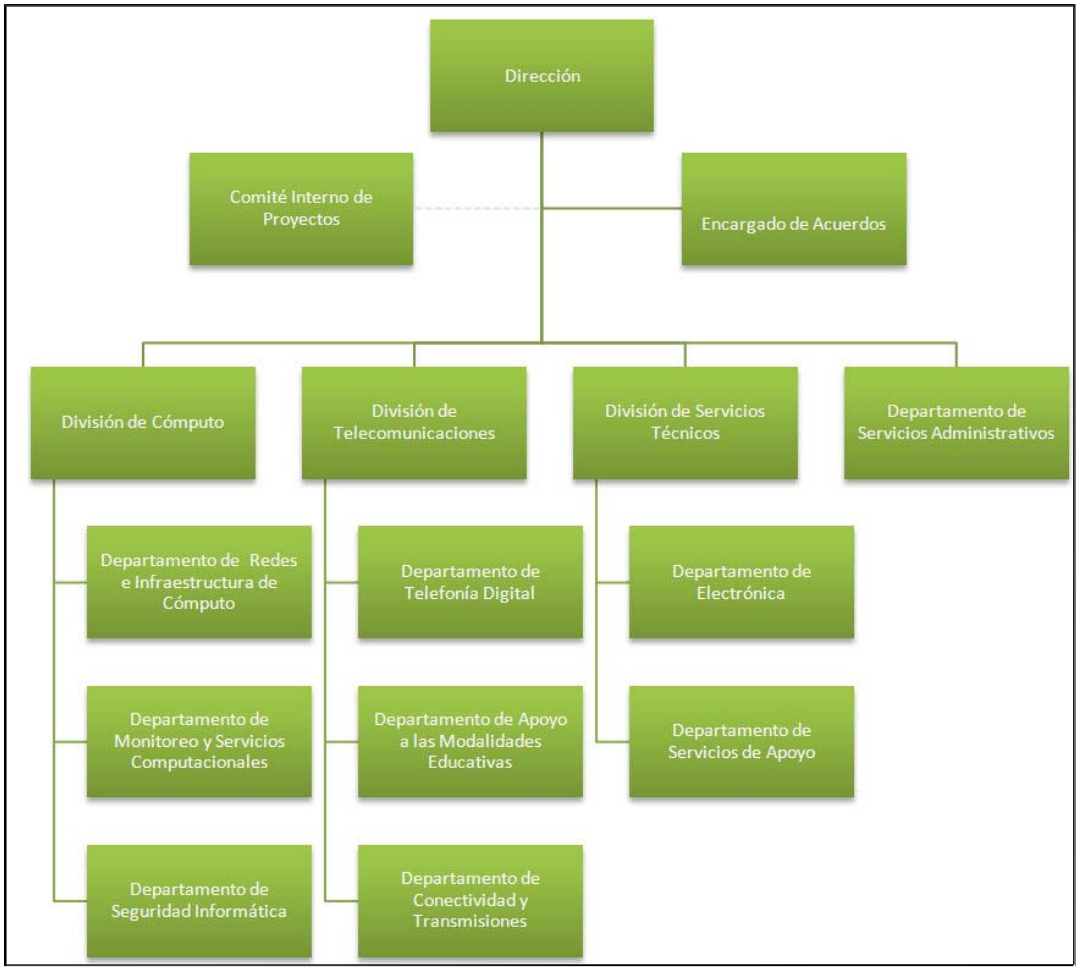
En 1994 se creó la Dirección de la Central Inteligente de Cómputo y Comunicaciones con el propósito de coordinar, operar y controlar las acciones del citado programa, misma que estaba integrada por doce órganos. En 1996 el Consejo General Consultivo del IPN aprobó la reestructuración orgánica del Instituto propuesta por el Director General, mediante la cual se modificó la denominación de la Dirección de la Central Inteligente de Cómputo y Comunicaciones a DCYC. Para 1998, y con el fin de que administrar a la entonces recién instalada red de telefonía, se creó el Departamento de Telefonía Digital, con lo que su estructura se incrementó a 13 órganos. En 1999, aumentó su estructura a catorce en virtud de que se autorizó la creación del Encargado de Acuerdos de la Dirección.

En 2001, mediante el Acuerdo DG/01/AG/01 emitido por el Director General se autorizó la estructura orgánica y funcional del IPN, publicado en los números 488 y 495 de la Gaceta Politécnica, y la DCYC cambió nuevamente su denominación a Dirección de Informática. En 2002, como resultado de una reorganización orientada al fortalecimiento y modernización de los servicios sobre la materia, se aprobó una estructura orgánica en la cual se reflejan los cambios de nomenclatura.

Posteriormente, en 2005 y derivado del Acuerdo por el que se aprobó la nueva estructura orgánico-administrativa de la administración central del IPN, publicado el 2 de septiembre en el número extraordinario 616 de la Gaceta Politécnica, se modificó nuevamente su denominación por la actual DCYC, quedando como lo

muestra la figura siguiente:

Figura 6: Estructura Organizacional DCyC



Fuente: Elaboración propia con base en los datos de la DCyC

Las actividades primordiales del Departamento de Seguridad Informática son: Administración de la Consola de Antivirus Institucional. Administración del Firewall/IPS Perimetral Institucional. Administración del Filtrado de Contenido Institucional. Implementación del NAC Institucional.

Es importante hacer notar que las funciones de creación y actualización de políticas y procedimientos de seguridad informática no están definidas debido a que aún no existen estándares de gestión de la seguridad de la información dentro del IPN.

El hecho de que la información se encuentra en todos los niveles de la Institución y no centralizada, hace que la interacción con el resto de las unidades departamentales sea constante y desgastante por las razones ya expuestas de la estructura formal. Aun así, la seguridad informática no radica únicamente en el Departamento de Seguridad Informática, pues encada ECU del IPN existe una UDI (Unidad de Informática) y su administrador es el encargado final de gestionar y vigilar el contenido de los servidores y los accesos al equipo de cómputo, la instalación de antivirus en los equipos institucionales, limitar la instalación de software de malicioso, así como de tramitar ante el área de seguridad los servicios a liberar para uso de la ECU que representan.

Las ventajas de segmentar las funciones en estructura lineal son:

- Línea directa de Autoridad
- Línea directa de comunicación
- Personal con alto gro de especialización.

Desventajas de este tipo de estructura son:

- Alta dirección absorbida por la operación
- Comunicación en un solo sentido
- Déficit de planeación
- Déficit de investigación
- Déficit de innovación

Como se mencionó en los capítulos anteriores, la importancia de considerar los efectos económicos y administrativos que conlleva la ausencia de seguridad informática dentro de las organizaciones crea una necesidad urgente de incorporar algunos métodos y herramientas que nos permitan gestionar la seguridad informática dentro de los sistemas de comunicaciones y cómputo alineados al cumplimiento de los objetivos Institucionales.

En un principio, por la propia naturaleza aislada de los sistemas de cómputo, se pensó que el hecho de recluirlos en sitios de acceso controlado los mantendría fuera de peligro como al parecer sucedía antes de la creación del DCYC. Aunque

esta situación era funcional para el IPN hasta principios de los noventa, en los años siguientes, y debido a los rápidos avances en el área de la informática, los sistemas de gestión de cómputo también evolucionaron y la primera innovación fue permitir las sesiones remotas obligando a los administradores de esos recursos a ajustar el diseño de sistemas de cómputo para que fueran capaces de mantener múltiples sesiones y administrar las tareas generadas por los usuarios. Además, las cambiantes arquitecturas en los sistemas operativos hicieron que se crearan nuevos roles de usuarios que necesitaban diferentes posibilidades de acceso a la información contenida en los sistemas, por lo que estos perfiles ahora obedecían a la política que el administrador del servidor aplicaba.

Bajo estos cambios, la intención del administrador no era proteger la información sino mantener un sistema organizado y con recursos disponibles para los usuarios. La mayor preocupación era el uso racional de los recursos de cómputo que en ese momento eran restringidos; la intención de ocupar mas capacidades de cómputo fue lo que llevo a las primeras infracciones de seguridad tratándose de apoderar de la mayoría de las conexiones, espacios en disco y capacidad de cómputo. Este auge motiva al usuario común a llevar sus programas a diferentes centros de cómputo y correr desarrollos en diversas plataformas despertando la necesidad de más recursos y mas velocidad en las comunicaciones también se desarrollan programas maliciosos de robo de contraseñas o inhibición de los equipos con el fin de no compartir esos recursos finitos.

Con el desarrollo de los sistemas de comunicaciones, las redes de datos permitieron el uso intenso y extenso de los sistemas mayores de cómputo abriendo las puertas a nuevas formas de acceder a las computadoras y poder ejecutar programas remotos de naturaleza maliciosa llamados virus. Los primeros virus modificaban la información volviéndola inútil, sin embargo, era compartida por pocos usuarios y el daño económico no llegaba más allá del pago de tiempo extra para la nueva captura de datos. No obstante, con el tiempo este tipo de daños evolucionaron y llegaron a convertirse en pérdida total de datos y en daño físico de los dispositivos de almacenamiento. Esta simple modificación levantó la alerta de

los directivos de empresas e Instituciones ya que los gastos en hardware eran muy fuertes y la innovación de los mismos dispositivos hacía imposible que se recuperara la información contenida en un lapso que las organizaciones pudieran absorber sin tener pérdidas de negocio o clientes insatisfechos que cambiaban de firma.

Los desarrollos tecnológicos de sistemas y hardware evolucionaron a tal ritmo que los servicios en tiempo real, las bases de datos, las páginas web, y el almacenamiento masivo se convirtieron en la preocupación de los directivos, en tal proporción que en 2004 el 63% de las organizaciones consideraba que la seguridad informática no era necesaria, por lo que no se planteaba la necesidad de un responsable de ella. Sin embargo, en 2007, el 85% de las organizaciones ya contaba con un oficial de seguridad de la información.

De las experiencias históricas las tres principales preocupaciones de los responsables de la seguridad de la información son, en orden de importancia: a) El uso de los dispositivos removibles, b) redes inalámbricas y c) la convergencia entre la seguridad lógica y física. Es importante mencionar que no quedan muy detrás el cómputo móvil, los dispositivos móviles de comunicación y las páginas web.

Para entender como ha crecido el impacto administrativo y económico se mencionaran las principales áreas en las que se apoya la seguridad informática:

Tabla 6 Cumplimiento de un SGSI en la DCYC

ÁREAS EN LAS QUE SE APOYA UN SGSI	CUMPLIMIENTO IPN
• Cumplimiento regulatorio	NO
• Alcanzar objetivos Institucionales	SI
• Privacidad y protección de la Información	SI
• Administración de riesgos Institucionales	SI
• Publicidad negativa	NO
•Phishing, spyware y amenazas técnicas	SI
• Riesgos con clientes	SI
• Nuevas tecnologías	SI
• Requerimientos de certificación de seguridad de la información	NO
• Riesgo relacionado con terceros	SI
• Riesgos relacionados con proveedores	SI

Fuente: Elaboración propia con base en información reservada de la DCYC**.**

Todos estos elementos necesitan del apoyo del comité de computo y comunicaciones, pues en caso contrario serán esfuerzos individuales, debido a los grandes huecos legales y de normatividad aunado a la falta de elementos que permitan lograr una cultura de seguridad informática entre los usuarios de tecnología, además de no existir una actitud proactiva dentro de las organizaciones.

De la misma forma que las instituciones trabajan en elementos que consideran pilares para poder ofrecer seguridad en sus transacciones los usuarios de tecnología informáticos y no informáticos solicitan de las empresas: capacitación, soporte técnico y asesoría.

Como lo señala la tabla siguiente, las principales preocupaciones del usuario para utilizar los servicios de cómputo y comunicaciones son:

Tabla 7 Vulnerabilidades previstas en un SGSI

Usuario General	PREOCUPACIÓN IPN
• Extracción de la información	SI
• Confidencialidad de la información	SI
• Robo de identidad	SI
• Pérdida de información	SI
• Integridad de la información	SI
• Uso de Banca Electrónica	NO
• Compras en Línea	NO
• Piratería como factores de riesgo	SI
•Pornografía	NO
•Obtención del servicio de Internet	SI
• Accesos inalámbricos	SI

Fuente: Elaboración propia con base en información reservada de la DCYC.

Como se puede ver en la tabla anterior, existe una gran preocupación de los usuarios en relación con la carencia de una adecuada gestión de la seguridad en los servicios de cómputo y comunicaciones. Por ello, el modelo de gestión que se propone para la Seguridad informática está basado en un enfoque racional para su desempeño y su mejora continua. En primera instancia se especifican una serie de requisitos para poder establecer las bases, al cual se le denomina "Plan". Una vez establecido el modelo se implementa y opera siguiendo los pasos de la fase "Do", Una vez implantado y en funcionamiento, el modelo se debe revisar y monitorear es la fase de "check".

Las diferencias entre las fases anteriores permitirán arrojar resultados para mantener y mejorar el modelo, procediendo a "actuar" tomando los correctivos necesarios. En cada una de estas fases se han colocado las condiciones correspondientes.

A continuación se propone un análisis de riesgo para dimensionar los elementos que pueden comprometer la operación de la DCYC.

4.1 Evaluación Teórica de Riesgo Informático en el IPN

Esta sección hará una evaluación teórica únicamente del nivel de riesgo informático que presenta el IPN debido a la ausencia de información puntual sobre el número e intensidad de los ataques que ha sufrido el Instituto, por lo que las cifras presentadas son sólo indicativas del riesgo que presenta la institución.

Se puede decir que una evaluación de riesgos sirve para identificar las amenazas, vulnerabilidades y riesgos de la información sobre la plataforma tecnológica de la institución referidos a los criterios de la seguridad informática, disponibilidad, confidencialidad e integridad de la información. Las referencias deberán ser proporcionadas por una serie de controles que aseguren un ambiente informático seguro.

La idea es poder identificar la probabilidad de una amenaza y si esta se convierte en un incidente poder identificar la magnitud de degradación en los criterios anteriormente mencionados.

La probabilidad de que la vulnerabilidad pueda ser explotada se puede clasificar de acuerdo a su naturaleza como: alta, media-alta, media, media-baja y baja. A continuación se describen estos riesgos.

Tabla 8: Fases de Riesgo Informático

Nivel	Definición
Alta=5	La amenaza es altamente motivada y es suficientemente capaz de llevarse acabo
Media-Alta=4	La amenaza está fundamentada y es posible
Media=3	La amenaza es posible
Media-Baja=2	La amenaza no posee una capacidad fuerte de materialización
Baja=1	La amenaza no posee la suficiente motivación y capacidad

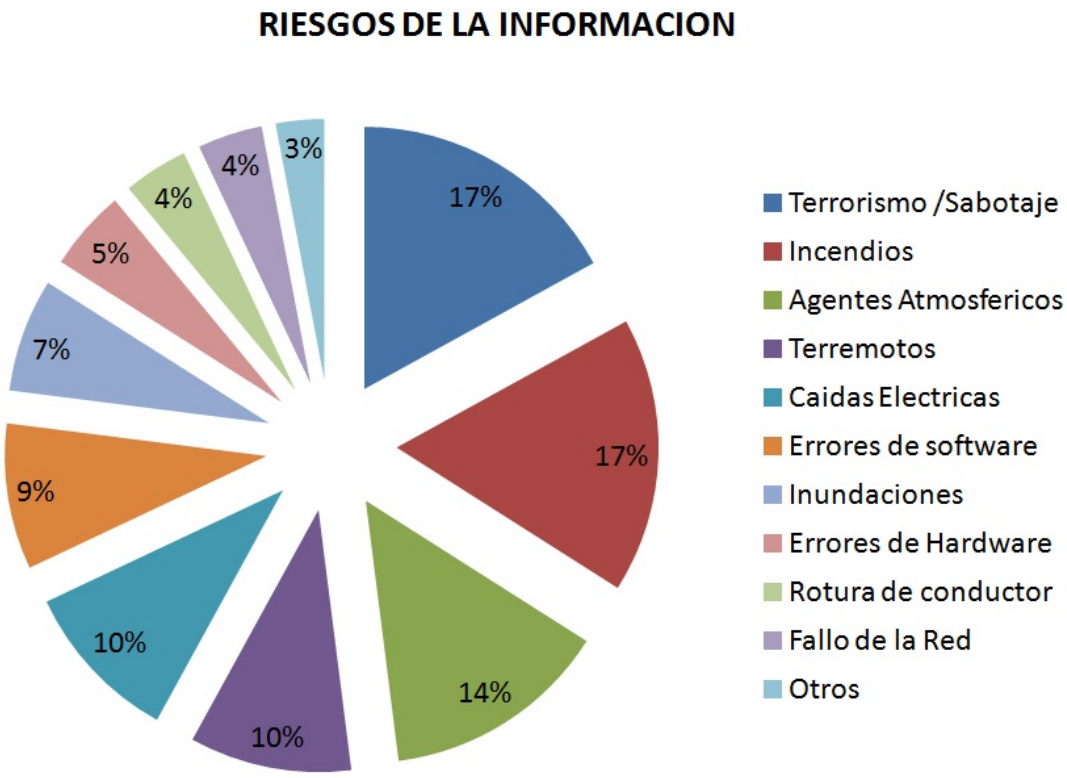
Fuente: Elaboración Propia

Para poder determinar la frecuencia de ocurrencia de un evento, se hará referencia a publicaciones tecnológicas como Information Week e Infosecurity

News[10] donde se pueden encontrar la mayoría de las estadísticas relativas a la información local e internacional para apoyar los casos de ataques informáticos que tenga registrados la institución.

Para el caso de la DCYC se utilizaran los datos aportados por Habeas Data México[11] en los que se reflejan los siguientes porcentajes históricos.

Figura 7 Porcentaje de riesgo en los SGSI



Fuente: Elaboración propia con datos de HD México

De acuerdo con este procedimiento, la ponderación que se deberá utilizar indica que si se tiene una probabilidad de vulnerabilidad alta (P=5) ésta no debe de presentarse por más de dos veces por año. Las demás serán en proporción al número de veces que pueda ocurrir el evento en ese mismo periodo de tiempo.

[10] véase las siguientes URL: http://www.cert.org, y http://www.sans.org
[11] Véase la URL http://www.hdmexico.com.mx

Identificación de vulnerabilidades

Para obtener este tipo de información se hará uso de un Checklist y de las herramientas informáticas que ayudan a determinar las vulnerabilidades de sistema operativo y de los sistemas de seguridad perimetral.

Seguridad Física:

- Monitoreo ambiental
- Control de acceso
- Desastres naturales
- Control de incendios
- Inundaciones

Seguridad en las conexiones de Internet

- Políticas en el Firewall
-
- VPN
-
- Detección de intrusos

Seguridad en la infraestructura de comunicaciones

- Routers
- Switches
- Firewall
- RAS
- Blindaje de Sistemas Operativos
- Correo electrónico
- Seguridad en las aplicaciones críticas: Estas deben ser analizadas en su conjunto, desde la generación del código, el sistema operativo, el servidor (Hardware), los dispositivos de

almacenamiento y respaldo, redes LAN y WAN hasta el centro de cómputo.

4.2 Componentes del Impacto y del Factor de Riesgo

El siguiente paso es poder determinar el impacto adverso para el IPN como resultado de la explotación de una vulnerabilidad inminente que se convierte en una amenaza y que puede tener efectos sobre cualquiera de las siguientes áreas:

Consecuencias de tipo financiero, es decir las pérdidas causadas a los activos físicos o lógicos de la organización y las consecuencias ocasionadas por la ausencia o mal funcionamiento de este elemento que afecte la continuidad del negocio o la operación de parte de ella.

La importancia de la criticidad del sistema y de los datos contenidos en él, ya que actualmente son factores críticos en una cantidad impresionante de transacciones lo que les otorga una gran importancia para la estabilidad y operación del sistema.

Ecuación del Análisis de riesgos basada en Ovsei Gelman

$$B>P*L$$

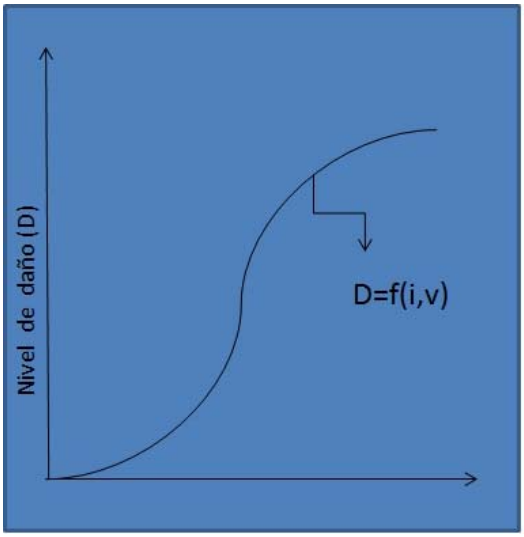
Donde,

B es el gasto que significa la prevención de una pérdida específica debido a una vulnerabilidad;

P es la probabilidad de que dicha vulnerabilidad sea explotada y ocurra una pérdida especifica de información;

L es el costo total que significa la pérdida específica de información debido a una vulnerabilidad que ha sido efectuada.

Figura 8 Curva típica de vulnerabilidad informática



Fuente: Elaboración propia basada en Gelman (2008)

Las dudas de cuándo y cuánto invertir en seguridad surgen al instante:

Si B≤P*L

Hay que implementar una medida de prevención. Dado que para el IPN la ecuación B>P*L implica que se mantiene un presupuesto para la mejora continua de la seguridad; sin embargo el peligro especifico de alta vulnerabilidad prevalece.

Sí B>P*L

No es necesaria una medida de prevención.

Cumpliendo con la condición de que no se puede invertir más dinero en la seguridad de un activo que el valor mismo del activo.

Las medidas y herramientas de control han de tener menor costo que el valor de las posibles pérdidas y el impacto de éstas si se produce la amenaza temida. Recordando la ecuación anterior; algo totalmente lógico es que tanto los directivos como los responsables de seguridad informática de las organizaciones deberán estimar de forma adecuada a su circunstancia. El verdadero problema es tener los elementos que permitan hacer un cálculo del impacto económico que se puede suponer del hecho de que ocurra una amenaza informática al sistema.

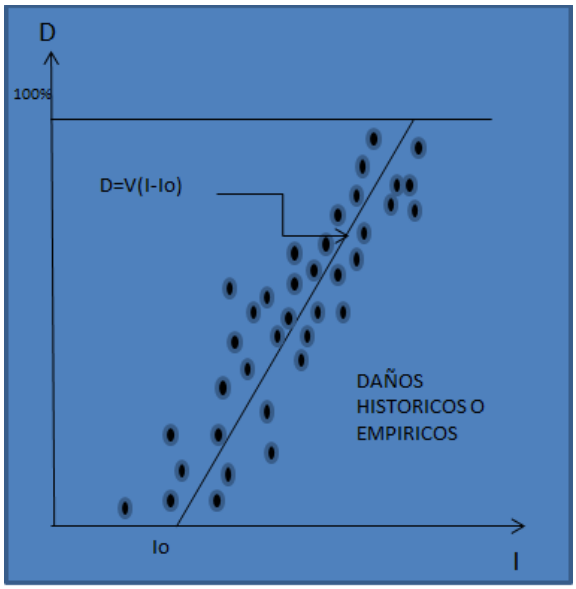
El factor de impacto L en B≤P*L es difícil de evaluar porque incluye daños a la

información, así como a los equipos de cómputo, pérdidas por reparación, el tiempo requerido para reiniciar el sistema, pérdidas por horas de trabajo, etc.

Siempre habrá una parte de valoración subjetiva, las pérdidas de datos pueden llevar a un efecto de cascada por el ser el principal insumo de los sistemas. Por ello se requiere de un grupo multidisciplinario capaz de ponderar todas las posibles pérdidas y cuantificarlas.

El factor P en B≤P*L está relacionado con la determinación del impacto total L y depende del entorno donde se presentó la amenaza. Las herramientas de probabilidad pueden asociar a una tendencia o frecuencia conocida para poder cuantificar esta variable especulativa. Una vez que se conoce P para un L dado, se obtiene la probabilidad de pérdida relativa de la ocurrencia P*L que se comprobara con B, el costo que nos supondría implantar la medida de prevención respectiva.

FIGURA 9. Ejemplo de evaluación de vulnerabilidad



Fuente *Gelman (2008)*

El factor B en B≤P*L Indica que se requiere para prevenir una pérdida de información. Puede ser la cantidad de dinero que vamos a disponer para mitigar dicha pérdida.

De acuerdo con las consideraciones señaladas arriba es pertinente preguntar ¿cuánta protección es necesaria en una organización? La respuesta dependerá del nivel de seguridad que la institución desee y que crea oportuna, o de los costos que imponga el entorno. Entonces también es pertinente preguntar ¿de qué forma se puede proteger la organización? La respuesta dependerá de las restricciones físicas, políticas de seguridad, controles de acceso, planes de contingencia y de recuperación, cortafuegos y las políticas de uso de cifrado, autenticación y firmas que tenga como objetivo dicha organización.

4.3 Restricciones de la Estructura Administrativa del IPN para la DCYC

De acuerdo a la Normatividad del IPN la Coordinación General de Servicios Informáticos es la autoridad superior que integra el Comité de Cómputo y Telecomunicaciones. Por disposición del Reglamento Interno del Instituto, sus escuelas, centros y unidades de enseñanza y de investigación adoptarán la organización académica, técnica y administrativa interna que establezcan la Ley Orgánica, siguiendo los principios generales de organización.

La DCYC, dependiente de la Coordinación General de Servicios Informáticos, amalgama las funciones de la convergencia tecnológica, cuyo objetivo es el de administrar y controlar los servicios de cómputo y comunicaciones que se proporcionan a la comunidad politécnica para desarrollar actividades académicas, de investigación, extensión, difusión, integración social y administración, mediante la aplicación de criterios de optimización, fortalecimiento, ampliación y modernización, en congruencia con el Programa Institucional de Desarrollo Informático.

Las UDIS, independientemente de lo que dispongan las políticas y lineamientos que emita la Coordinación, tendrán las siguientes obligaciones:

I. Implantar y vigilar las políticas de seguridad de la infraestructura de cómputo y telecomunicaciones al interior de las dependencias politécnicas de que se trate.

II. Verificar el software especializado y de uso específico que se instale en los equipos de las dependencias politécnicas de su adscripción y que esté destinado a dar servicio a los usuarios, tales como compiladores, intérpretes, bases de datos, sistemas operativos o paquetería.

III. Vigilar que la instalación de software se realice sólo cuando se cuente con el licenciamiento correspondiente y del que se tenga la seguridad de que no representa riesgos para la integridad de los equipos y sistemas ni para la Red Institucional.

IV. Bloquear las cuentas de usuarios en aquellos casos en los que no hayan sido utilizadas por periodos prolongados, exceso de intentos fallidos al tratar de abrir una sesión y accesos a páginas no autorizadas en términos de los privilegios asignados al usuario.

V. Mantener informada a la Coordinación cuando concurran cualquiera de las siguientes situaciones:

a) Actualizaciones o cambio de versiones realizadas a sus sistemas operativos.

b) Actualizaciones de seguridad aplicadas al sistema operativo.

c) Habilitación de nuevos servicios.

d) Ataques e incidentes observados;

e) Virus detectados.

f) Modificaciones mayores de configuración, tales como cambio de dirección, cambio de nombre, de dominio, entre otros.

g) Del desarrollo de los proyectos de expansión de servicios de voz y datos, cuando se construyan nuevos edificios u oficinas de las dependencias politécnicas de su adscripción, mismos que se realizarán conjuntamente con la Coordinación.

VI. Llevar una bitácora de incidentes de seguridad, la cual incluirá información relacionada con incidentes presentados como ataques, negación de servicio, robo de cuenta.

VII. Contar con un plan de contingencias que permita en casos críticos la

recuperación del sistema, herramientas e información de los servicios a su cargo.

VIII. Consultar a la Coordinación sobre los servicios que puede instalar en su servidor.

IX. Permitir el acceso al personal técnico especializado de la Coordinación cuando se presenten incidentes graves de seguridad, así como implementarlos procedimientos o medidas que le indique la propia Coordinación para corregir y evitar problemas.

X. Mantener disponibles los croquis actualizados de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red y tener y mantener actualizadas las listas de control de acceso a los servidores bajo su responsabilidad.

XI. Las demás que se requieran para el adecuado funcionamiento de la Red Institucional en las áreas de su competencia.

Las UDIs, conjuntamente con la Coordinación, deberán instalar y utilizar periódicamente las herramientas de software validadas por esta última, para detectar posibles fallas de seguridad y, en su caso, corregirlas en sus sistemas.

De acuerdo con el artículo 43 del Reglamento Interno del IPN, las UDIs limitarán sus acciones de seguridad informática al interior de las dependencias politécnicas a las que se encuentren adscritas.

En caso de que utilicen herramientas de este tipo sobre otros servidores o equipos de comunicaciones fuera de su área de responsabilidad, estas acciones serán consideradas como ataques a la Red Institucional y estarán sujetas a las sanciones correspondientes. [12]

[12] Revisar GACETA POLITÉCNICA, reglamento para la operación, administración y uso de la red institucional de computo y telecomunicaciones del IPN: artículos.41,42,43.

4.4 Análisis FODA de la DCYC

A continuación se presenta un cuadro con el análisis de las principales fortalezas, oportunidades, debilidades y amenazas (FODA) de la DCYC.

Tabla 9: Análisis FODA de la DCYC

FORTALEZAS ***F1*** Infraestructura consolidada ***F2*** Asignación por rol funcional ***F3*** Conocimiento de la problemática ***F4*** Capital Humano ***F5*** Liquidez económica para nuevos proyectos ***F6*** *Disposición* de los encargados	***DEBILIDADES*** ***D1*** Falta de liderazgo ***D2*** Falta de personal ***D3*** Rotación de Personal ***D4*** Perfiles no adecuados ***D5*** Falta de capacitación ***D6*** No existe planeación ***D7*** Falta de procesos ***D8*** No se genera información ***D9*** No existen métricas ***D10*** No existe difusión ***D11*** Nula vigilancia tecnológica
OPORTUNIDADES ***O1*** Capitalizar el conocimiento adquirido a través del tiempo por el personal ***O2*** Implantar mejores prácticas del mercado ***O3*** Crear contenidos académicos de seguridad de la información ***O4*** Sinergia ***O5*** Mantener una imagen de respeto ***O6*** Gestionar nueva infraestructura de seguridad Informática ***O7*** Aumento de las aplicaciones web 2.0 ***O8*** Mitigar la variación y dispersión de esfuerzos	***AMENAZAS*** ***A1*** Falta de organización ***A2*** Compatibilidad cultural ***A3*** Compatibilidad tecnológica ***A4*** Daño a la imagen Institucional ***A5*** No comprender la importancia del departamento ***A6*** Pérdida de credibilidad ***A7*** Outsourcing de seguridad ***A8*** Menor número de proyectos vinculados ***A9*** Recorte de Presupuesto ***A10*** Recorte de Personal ***A11*** Cloud computing ***A12*** Incapacidad para enfrentar la demanda por servicios

Fuente: Elaboración propia

A continuación se describen de manera pormenorizada dichas evaluaciones:

OPORTUNIDADES

O1. –La creación de capital humano de calidad es una ventaja competitiva de la unidad de Seguridad informática, la resolución de incidentes diarios de casi 20 mil usuarios ha permitido que el conocimiento del personal técnico sea muy elevado y este conocimiento se trasmite a través del servicio social, en forma personalizada pudiendo conservar este capital intelectual generando procedimientos acerca de los tópicos enfrentados diariamente.

O2. -La oportunidad que tiene el IPN al estar integrada a la ANUIES permite una gran diversidad de intercambio de experiencias sobre problemas de seguridad de la información y las soluciones que se les han encontrado, en ese mismo ámbito, el departamento de seguridad informática podría acercarse a modelos de estandarización internacional o mejores prácticas que den certeza del manejo que se hace la infraestructura de computo y comunicaciones por lo menos a nivel seguridad, aunque no estaría de más que la Dirección completa se apegará a un solo estándar.

O3. - Dentro del IPN existen esfuerzos por integrar este conocimiento a la vida académica, pero la seguridad de la información se encuentra en toda la institución por lo que la creación de material académico para todo nivel es una oportunidad de difundir la cultura de seguridad informática y hacerse de prestigio y recursos.

O4. - Aprovechar las recomendaciones de Cómputo y Comunicaciones para enriquecer las labores cotidianas e impulsar nuevos proyectos con la sinergia de las distintas áreas operativas con una sola causa.

O5. - La consolidación de un departamento de seguridad informática que tenga la suficiente difusión y argumentos para competir a nivel resolutivo e innovador con dependencias educativas, gubernamentales y privadas enfocadas a la seguridad de la información.

O6. –En un sistema con demandas cambiantes por parte de la comunidad estudiantil, como de la sociedad misma es necesario mantener una infraestructura de seguridad informática versátil, maleable para adoptar nuevos contenidos sin poner en riesgo la información que se genere o se transmita por las aplicaciones nuevas.

O7. –El aumento de aplicaciones en la web 2.0 genera un gran volumen de información personal y de información compartida en tiempo real, de tal forma que la generación de material para estos espacios requiere de una disponibilidad de red casi del 100%, a cambio la imagen de vanguardia y de apertura contribuirán a la integración de más usuarios y más información circulando por la comunidad estudiantil.

O8. - Es deseable la unificación de criterios y el aumento de la cultura informática por medio de la transferencia tecnológica que se derramará en la comunidad politécnica impulsada por el uso de nuevas tecnologías de TI, tanto en la administración como en su generación y uso.

09.-Outsourcing como una medida para compartir el riesgo y una forma eficaz de transferencia tecnológica, para las áreas cuyo ámbito es la frontera tecnológica.

AMENAZAS

A1. –Falta de una planeación, con estrategias y objetivos bien definidos que sean difundidas y entendidas por las ECUs.

A2. - Se deben generar espacios para la difusión de la cultura en seguridad informática, evitar que la comunidad la perciba como impedimento de trabajo o libertad sino una herramienta para mantener los servicios de red disponibles.

A3. -Lo servicios de TI que se ofrecen no han cambiado y no se ha impulsado el cambio tecnológico en servicios que están disponibles en otras instituciones y que la comunidad demanda para su conocimiento y uso masivo.

A4. - Los usuarios tienen un desconocimiento de las actividades del departamento de seguridad informática, teniendo como resultados un sentimiento de inseguridad

informática en el mejor de los casos, el peor escenario es la no utilización de los servicios informáticos institucionales.

A5. – Es importante no desgastar la imagen del departamento de seguridad informática al difundir de forma institucional solo aquellos casos donde fue vulnerada, restándole certeza y credibilidad a su trabajo.

A6. - La debilidad de una organización es igual a la de su elemento más vulnerable, reforzar la imagen de un departamento reafirma la imagen de la institución.

A7. - Entre otras existe la figura de *outsourcing* (subcontratación) para solventar los daños a la imagen y credibilidad institucional evidenciando la incapacidad de respuesta interna, situación impensable en una institución de educación especialista en el área de ciencias. Personal de empresas especialista realiza el trabajo que el personal de estructura no puede realizar por falta de experiencia ó desconocimiento tecnológico.

A8. - Los proyectos vinculados con otras instituciones de gobierno y privadas posicionan a la imagen Institucional evidenciando el uso de "la técnica al servicio de la Patria" promoviendo los servicios de TI que el IPN tiene disponibles a la sociedad. Lamentablemente las constantes interrupciones en la disponibilidad de estos servicios han limitado el uso y utilización de estas tecnologías.

A9. –Las opiniones de que los servicios de TI no sirven pueden encontrar eco, dejando de invertir en la infraestructura de cómputo, comunicaciones y seguridad. El desarrollo vertiginoso de las ECUs en estos tópicos, ha permitido el desarrollo de sus propios mecanismos de conectividad y seguridad; dependiendo cada día menos de la interacción con el área central, es otro escenario que no se descarta cuestionando entonces la existencia operativa del área central.

A10. – Con estos antecedentes y pese a la automatización de los sistemas de TI es necesario contar con más personal con el perfil adecuado capaz de brindar una atención más cercana a las diferentes ECUs reforzando la identidad y fortaleciendo la confianza.

A11. - Es una realidad que muchos servicios tienen mayor capacidad y disponibilidad en la nube de internet, la única deficiencia es la seguridad que ofrecen (por el momento) ya que nadie garantiza que esa información no se pierda, en cambio las instituciones de educación, si pueden ofrecer esa garantía hasta cierto límite, sin costo directo para la comunidad Institucional.

A12. - Las necesidades de cómputo son dinámicas y la conectividad tiende a ser gratuita mejorando las velocidades de acceso a internet por lo tanto la conectividad ya no será el problema, en cambio la seguridad se mantendrá como un elemento indispensable en la administración de las TI haciendo evidente continuar con su innovación y generación de capital humano a través de una correcta transferencia tecnológica.

FORTALEZAS

F1. - Existe una constante inversión en proyectos de conectividad y capacidad de cómputo para el Instituto.

F2. –La asignación de encargados de los diferentes sistemas de seguridad ha permitido por su continuidad mayor a dos años la creación de capital humano y una capacitación personalizada que se incrementa con cursos de entrenamiento impartido por los fabricantes.

F3. - El personal conoce la problemática salarial, social y de personal mostrando una gran disposición y un continuo auto aprendizaje, forjándose un carácter con temple y actitud de servicio.

F4. - La transferencia tecnológica que recibe el personal y que se replica a los becarios de servicio social genera un capital humano de excelente capacidad que tiene garantizada la inserción en el mercado de las TI.

F5. – En la medida que ha surgido una serie de propuestas en cualquier departamento que signifiquen una innovación tiene el apoyo de las autoridades para su implementación en proyectos que por su tamaño pueden ser multianuales.

F6. – Los encargados de los sistemas de seguridad tienen la disponibilidad de

implantar sistemas que han sido solicitados por otros departamentos sin conseguir su implementación, el objetivo se cumple al ponerlos en marcha, aun cuando eso signifique el aumento de horas de trabajo e investigación.

DEBILIDADES

D1. – Dada la cantidad de personal que en su mayoría realiza trabajo operativo para lograr los objetivos de la Dirección, no se realizan actividades de monitoreo tecnológico. Las innovaciones no son impulsadas por el departamento de Seguridad informática, la falta de una metodología de benchmarking respecto a su entorno no le permiten presentar una prospectiva de seguridad informática que sea tomada en cuenta de forma definitiva. Esta actividad la realizan las divisiones de computo y comunicaciones respectivamente y el departamento solo aplica las que le sean asignadas provocando duplicidad de roles y funciones.

D2. - Existe una dependencia real de los encargados de los sistemas de seguridad informática, en virtud de la falta de personal de estructura que tenga un contacto estrecho con el manejo de los sistemas y del apoyo de documentación de procesos también inexistente.

D3. - La movilidad de personal está presente por falta de incentivos económicos y seguridad debido a los que un porcentaje del personal está bajo el régimen de becas, interinatos u honorarios.

D4. - Existe personal que no cumple con el perfil que corresponde a estas actividades, dejando la responsabilidad operativa y de documentación a los encargados.

D5. - No existe un programa anual de capacitación.

D6. – Estas ausencias denotan una falta de estrategia y tácticas adecuadas para enfrentar los problemas de forma adecuada.

D7. – Los incidentes se pretenden resolver por un procedimiento general, no documentado y que depende de la experiencia de los encargados, esa experiencia estriba en gran medida de la memoria del encargado, resolviendo un mismo

problema de diferentes formas y no por la idónea.

D8. - No se genera un intercambio de conocimiento con la comunidad a través de las TI, en las que se plasmen procesos que pudieran ayudar a mitigar la inseguridad de sistemas utilizados por los usuarios.

D9. - No existen indicadores que permitan conocer el nivel seguridad información que percibe la comunidad en general respecto a los servicios informáticos que ofrece el IPN.

D10. - No existe un programa de difusión de seguridad informática, en el cual se difundan las mejores prácticas de seguridad, recomendaciones sobre el uso de herramientas informáticas y riesgo potencial entre otros.

D11. - No existe un programa de vigilancia tecnológica, que permita conocer y comparar las diferentes soluciones de seguridad que tengan mercado y cuáles de ellas en realidad representa una innovación.

Del análisis anterior se desprende que la DCYC presenta varias deficiencias organizacionales con respecto a los modelos teóricos discutidos en el capítulo anterior. Es importante hacer notar que la propia actividad tecnológica de la DCYC la acerca al perfil definido por Woodward, por lo que la influencia de los cambios tecnológicos en las plataformas que opera el IPN afecta directamente a la manera en la que tiende a operar la DCYC, lo cual implica la aparición de un efecto externo sobre su propia organización. Sería deseable, por lo tanto, que las autoridades del IPN tomarán en consideración este tipo de influencias para gestionar una estructura más flexible que le permitiera a la DCYC actuar con rapidez en el evento de una amenaza a la estabilidad de las plataformas informáticas de la institución.

CONCLUSIONES

En los últimos años el tema de la seguridad informática ha venido teniendo una presencia cada vez más importante dentro de las instituciones como resultado del auge en las actividades derivadas de las TIC, pero mucho de este crecimiento se debe, paradójicamente, a la oferta de aplicaciones informáticas que se presentan en extramuros. Esto porque la facilidad de intercambiar información en cualquier parte del mundo trae también desventajas en cuanto a la propiedad industrial e intelectual, obligando a que las instituciones tengan que orientar a sus usuarios sobre cómo usar y manejar estas herramientas, evitando así el mal uso de los recursos. En el caso del IPN, el riesgo de un mal manejo de los recursos informáticos se puede materializar en el deterioro de los medios y servicios que el instituto oferta a la comunidad en primera instancia.

Para tener mecanismos de gestión funcionales es imprescindible partir de una política que pueda incluir todos los elementos que por sí mismos son dinámicos dentro del contexto de la seguridad informática, y no solamente construir reglamentos técnicos ni estrategias legales, sino un compromiso institucional de una renovación constante ya que los elementos a revisar giran en torno a las TIC que sufren constantemente cambios por moda y otras más trascendentes referentes a la regulación del gobierno.

Hay que destacar que una política de seguridad informática es una forma de establecer una comunicación con los usuarios mediante el diseño y aplicación de reglas claras en el uso y aplicación de los recursos informáticos de la organización. Más aún, una política funcional de seguridad informática debe considerar los siguientes elementos: 1) Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. 2) Objetivos de la política y descripción clara de los elementos involucrados en su definición. 3) Responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización. 4) Requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política. 5) Definición de violaciones y sanciones por no

cumplir con las políticas.

Asimismo, La política de seguridad informática tiene implicaciones mas allá de las instituciones, más allá de los grupos de poder, pues en un mundo globalizado la imagen de las TIC vienen por definición acompañados de la seguridad o la inseguridad. De esto depende la percepción de la sociedad porque la mayoría de las veces está en juego la reputación de la Institución, y en algunas otras la trayectoria administrativa y académica de los dirigentes, pero finalmente dependerá de las circunstancias cotidianas, la disponibilidad de los servicios, su capacidad de almacenamiento, la velocidad de respuesta en la interacción entre las diferentes formas de comunicarse en las que tengan una presencia activa las instituciones para formarla huella deseada de que se proporcionan servicios seguros, y que ésta se traduzca en calidad.

En términos de su diseño, existen características deseables en una política para que pueda ser llevada a cabo. Tales características son: debe ser holística, es decir, debe cubrir todos los aspectos relacionados con la misma; debe ser atemporal; debe adecuarse a las necesidades y recursos; y debe definir estrategias y criterios generales a adoptar en distintas funciones y actividades, donde se conocen las alternativas ante circunstancias repetidas. Así como proporcionar las condiciones requeridas para garantizar la seguridad informática, tales como la integridad, la disponibilidad, la privacidad, y adicionalmente, control, autenticidad y utilidad.

De esta forma, la política de seguridad informática no debe ser un manual de dispositivos de seguridad, tampoco un elemento coercitivo que desmotive la utilización de las TIC, sino una descripción de los activos que se desean proteger y el porqué de ello.

En el caso del IPN, su estructura organizacional permite un primer acercamiento al análisis de la seguridad informática mediante el reglamento vigente para el uso de los servicios informáticos, el cual establece restricciones formales a la comunidad politécnica sobre el uso de los mismos, buscando una corresponsabilidad informal de reciprocidad en aras de de mantener los servicios disponibles para la misma comunidad fuera del perímetro territorial del IPN.

Este reglamento se basa en un sistema de incentivos dirigidos a los diversos servicios que son obtenidos por el buen manejo y responsabilidad en el uso de los activos informáticos, aunque también establece castigos en caso de un mal uso de los recursos.

No obstante, al ser el IPN una institución sujeta a las grandes transformaciones del país, también requiere de ajustes, y especialmente en un área tan delicada como es la de los servicios informáticos. El cambio institucional emprendido en la presente administración refleja las demandas de la comunidad politécnica en términos de la protección efectiva de su privacidad. De ahí que estos cambios partan de la creación de la unidad de seguridad informática, surgida de la reestructuración de 2005; siendo evidentes estos cambios en julio de 2006 cuando se emite la guía que la Institución proporciona a la comunidad para que a través de "El reglamento para la operación, administración y uso de la red Institucional de Cómputo y Comunicaciones del IPN " publicada en la Gaceta Institucional se conocieran las restricciones formales e informales respecto al uso de los sistemas de enseñanza, la producción y organización Institucional.

Este reglamento también modificó las condiciones para el uso de los sistemas basados en las TIC, el cual será clave para el desarrollo futuro del IPN en materia de seguridad informática.

Sin embargo, un elemento faltante en este esquema es el desarrollo de un marco estratégico tecnológico que se encuentre alineado con los objetivos del instituto, y que se traduzca en la elaboración de una cartera de proyectos de gestión de la seguridad informática que vayan más allá de la implementación de actividades correctivas cuando se presentan eventos de riesgo.

Para ello es imprescindible contar con un capital intelectual en la DCYC que sea más que la simple suma de los elementos que la integran y que sea capaz de crear las conexiones adecuadas para generar servicios de valor para la comunidad. Siendo el conocimiento una fuente de generación de ventajas competitivas, el IPN debe desarrollar su capacidad para identificarlo, medirlo, gestionarlo y en su caso protegerlo. La administración debe reflexionar sobre los fracasos previos y revisar

las experiencias generadas en esos entornos para poder captar el conocimiento pertinente de la experiencia.

Asimismo, se debe privilegiar los elementos del servicio que vayan dirigidos a detectar oportunidades, tomando como base de apoyo las capacidades organizacionales, para generar productos, procesos y servicios informáticos novedosos para la comunidad del IPN. Esto implica un compromiso de mejora, que se convierta en una actividad recurrente y modificatoria sobre los procesos y servicios ofrecidos por la DCYC que presenten ventajas en el desempeño, mejorasen la calidad y disminución en los costos.

Es importante hacer notar que el IPN no está ajeno a las fuerzas que ha identificado la teoría institucionalista con relación al efecto que tienen las directrices del Estado en cuanto a que sus acciones tienden a crear sistemas administrativos en donde la burocracia afecta la conducta entre las distintas instancias de control y operación. El ejemplo más claro de esta situación lo encontramos en la falta de coordinación que debería existir entre la política federal acerca de la llamada "agenda digital" y la instrumentación de dicha política en el ámbito del Programa Institucional de Desarrollo informático y las directrices y reglamentos que se emiten dentro del IPN.

Stiglitz (2006) observa que las instituciones por su naturaleza y tamaño no siempre son eficaces para vincular la realidad social y económica con la tecnológica, siendo muchas veces rebasadas por la sociedad civil; lo que pone en evidencia que las instituciones no siempre son capaces de cumplir con los objetivos deseados y de responder a las expectativas para los cuales fueron creadas. Es, entonces, cuando es conveniente redefinir el marco institucional y, en su caso, proponer nuevas estructuras que respondan de manera más efectiva a las necesidades de la sociedad.

En este contexto, en los capítulos anteriores se habló de la estructura y de los recursos con los que cuenta la DCYC, para lo que se realizó un análisis FODA, cuyas implicaciones para la operación de la Dirección de Cómputo y Comunicaciones serían: 1) Identificar los procesos críticos, las aplicaciones y la infraestructura tecnológica que soportan sus actividades en el entorno de su

operación. 2) Hacer un levantamiento topológico detallado de la infraestructura tecnológica existente, en el que se especifique y detalle la plataforma de hardware, software, comunicaciones y procesos utilizados por el IPN, y 3) Hacer una lista de verificación de la infraestructura tecnológica.

Este checklist serviría para identificar las vulnerabilidades de las plataformas tecnológicas.

A continuación se proponen veinte adecuaciones a las actividades sustantivas del área de cómputo del IPN con la finalidad de mejorar su capacidad de gestión de los riesgos informáticos:

1. Establecer las responsabilidades de seguridad de la información en todas las aéreas orgánicas del Instituto de forma escrita;

2. Establecer una política de seguridad de la información alineada en un principio a estándares internacionales y las mejores prácticas del mercado;

3. Establecer un modelo mínimo de gestión de la seguridad informática que permita alcanzar objetivos específicos en corto plazo;

4. Definir los procesos relacionados con la seguridad de la información tendiente a una mejora continua;

5. Definir y documentar metodologías para la resolución de contingencias;

6. Difundir aspectos básicos de seguridad de la información a la comunidad del IPN;

7. Implementar controles para las diferentes tecnologías que utiliza el IPN;

8. Auditar el cumplimiento de la política de seguridad Institucional;

9. Mitigar y analizar incidentes de seguridad (análisis forense);

10. Establecer períodos de evaluación de vulnerabilidades por sistema, tecnología y rol de actividades;

11. Evaluar los tiempos de vida tecnológicos de las soluciones de seguridad de la información a todo nivel;

12. Tener un estrecho contacto con el comité de programa de cómputo y

comunicaciones;

13. Solicitar a los responsables de los activos del IPN las políticas de protección, perfiles de acceso, respuesta a incidentes en períodos trimestrales;

14. Crear y administrar una base de datos común de los activos del Instituto clasificados por servicio, responsable, nivel de riesgo, antigüedad tecnológica y nivel de capacitación;

15. Coordinación y asesoramiento con los órganos administrativos que se relacionan con la identidad, seguridad física, y seguridad de la información para medios no digitales;

16. Desarrollar y administrar el presupuesto de la seguridad de información Institucional;

17. Emitir reportes periódicos del estado de seguridad de la información de la Institución por medios electrónicos y por escrito a la DCYC;

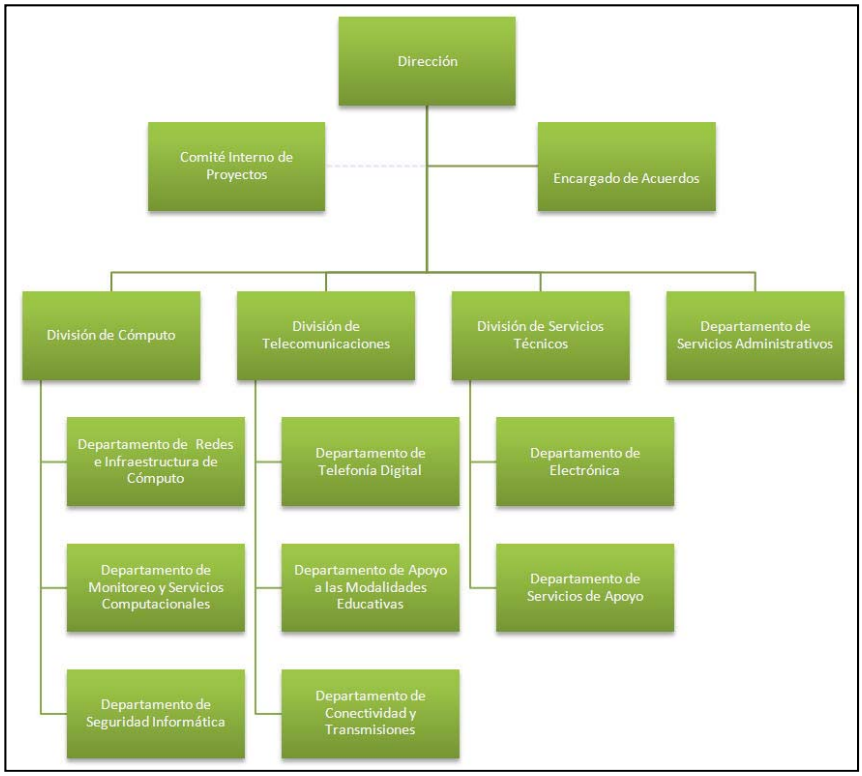
18. Establecer las acciones de penalización por infracción o desatención del reglamento de Seguridad Informática;

19. Monitorear permanente las aplicaciones disponibles para la comunidad del IPN y la sociedad en general;

20. Controlar aspectos de seguridad en el intercambio de datos entre los órganos del IPN y las diferentes entidades con las que se tienen convenios de colaboración tecnológica y comercial;

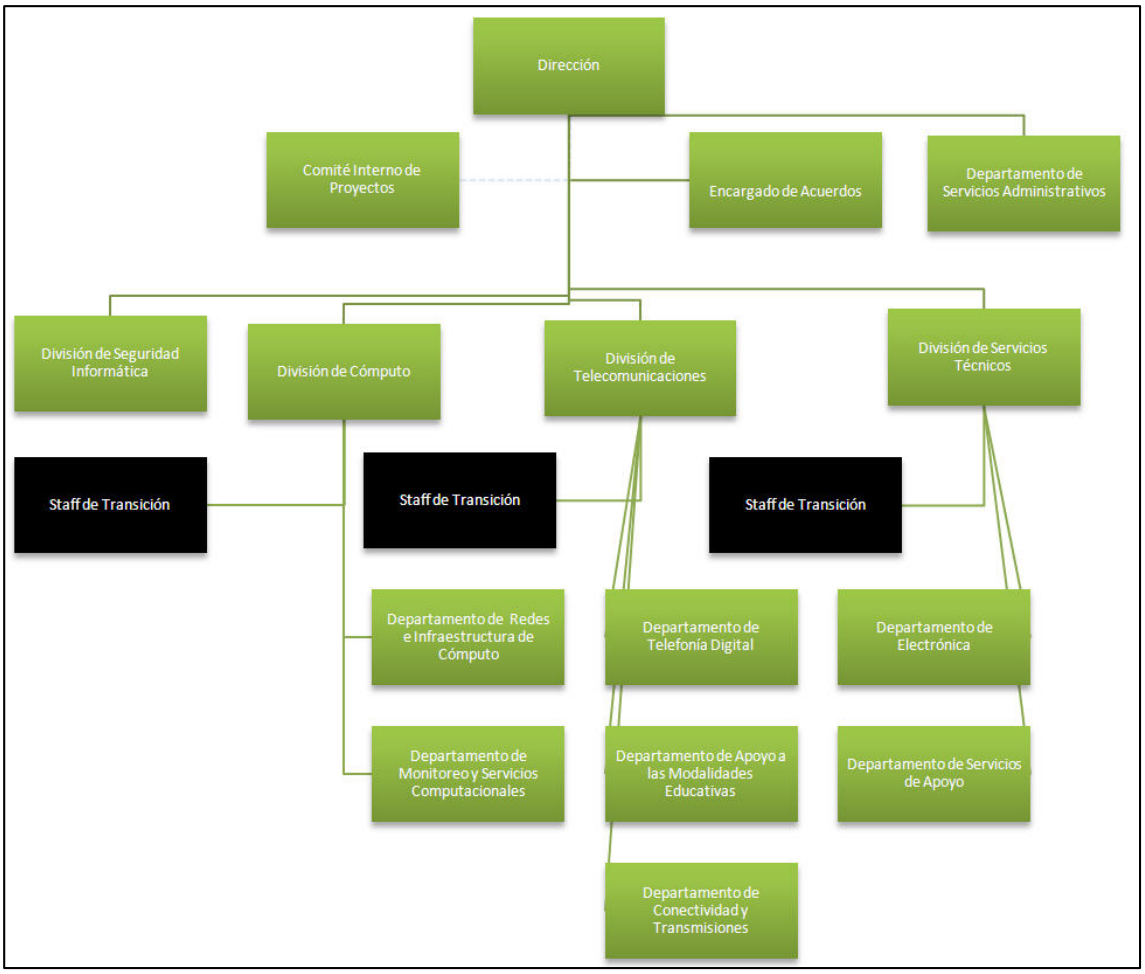
Es obvio que la implementación de estas adecuaciones requiere cambios en la estructura organizacional de la DCYC, que respondan de manera más eficiente y efectiva a sus necesidades de operación y que mejoren el desempeño de sus áreas funcionales, especialmente en relación con la ubicación geográfica de las actividades. La figura siguiente presenta el organigrama actual de la DCYC.

Contraste Organigrama DCYC –Propuesta Organizacional



Conforme a la discusión abordada en esta tesis, la figura siguiente presenta una propuesta de modificación a la estructura organizacional de la DCYC.

Figura 10: Organigrama Propuesto para la DCYC



Fuente: Elaboración propia

De las actividades descritas arriba, es evidente que el área de Seguridad Informática no debe permanecer más en la línea directa de Cómputo y que sería recomendable elevar su rango a División de Seguridad de la Información.

Esta transición requiere tanto de elementos de formalidad, líneas de mando, un perfil adecuado, una curva de aprendizaje, así como de los procesos de entendimiento y asimilación de responsabilidades, los roles que en una primera etapa funcionaran como staff y que a medida de la coordinación podrán ser ejecutados de manera formal apoyados por la correspondiente línea de mando.

Tomando como base las preguntas que se plantearon al inicio de esta tesis,

podemos decir que, en su estado actual, la seguridad informática es un aspecto que no es atendido de manera prioritaria por las administraciones del IPN, por lo que la gestión del cambio tecnológico en la seguridad informática en la DCYC es todavía una asignatura pendiente de resolverse, y por ende, su influencia en la comunidad del IPN es aún poco perceptible.

De implementarse los cambios propuestos en este trabajo, es probable que el manejo y gestión de los riesgos informáticos en el IPN experimente una mejora considerable y que los usuarios obtengan mayores beneficios de la infraestructura con la que cuenta el Instituto.

BIBLIOGRAFÍA

Abell, D. F. (1980) *Defining the Business*, Englewood Cliffs, Prentice-Hall.

Alexander, A. (2007) *Diseño de un Sistema de Gestión de Seguridad de Información*, México, Alfaomega.

Anderson, J. P. (1980) *Computer Security: Threat Monitoring and Surveillance*, Boca Raton, ICS.

APM Group (2008) "Information Technology Infrastructure Library (ITIL)", recuperado el 23-09-2008 de la URL: www.itil-officialsite.com/AboutITIL/WhatisITIL.asp

Ardita, J. C. (2010) Director de Cybsec S.A. Security System y ex-Hacker. Entrevista personal realizada el 15 de enero de 2010 en instalaciones de Cybsec S.A. [http://www.cybsec.com]

COBIT (2008) Tech Target, disponible en la URL: http://searchdatacenter.techtarget.com/sDefinition/0,sid80_gci5355709,00.html [recuperado el 23-09-2008]

COTEC (1999) "Modulo II" en *Herramientas de Gestión de la Tecnología*, Madrid, Fundación COTEC para la Innovación Tecnológica.

Ergas, H. (1987) "The importance of technology policy", en Dasgupta, P. y P. Stoneman (eds.) Economic Policy and technological Performance, London, Centre for Economic Policy Research, pp. 51-96.

Escorsa, P. y J. Valls (2001) *Tecnología e Innovación en la Empresa: Dirección y Gestión*. México, Alfaomega.

Fernández, C. M. (1988) *Seguridad en sistemas Informáticos*. Ediciones Díaz de Santos S.A. Madrid.

Gerwin, D. (1971) "Relationships Between Structure and Technology at the Organizational and Job Levels, "*Journal of Management Studies*, vol. 16 (1): 70-79.

Grupta, N. (1980) "Some Alternative Definitions of size", *Academy of management Journal*, December 1980, pp. 761-778.

Hidalgo, A., G. León y J. Pavón (2002) *La Gestión de la Innovación y la*

Tecnología en las Organizaciones. Madrid, Pirámide.

Holbrook. J (1991) Site Security Handbook, New York, J. Reynolds.

Huerta, A. (2006) "Seguridad en Unix y redes. (Versión 1.2), México, McGraw-Hill.

International Standards Organization (ISO) Norma ISO/IEC 17799; BS 17799 [recuperada en la URL: http://www.insi.org/BoletinInformativoISO27001.pdf]

Instituto Politécnico Nacional (IPN) (2006) *Gaceta Politécnica*, Año XLI Vol. 9 Núm. 633.

Jorgenson, D. W. y C. W. Wessner (Eds.) (2006) *Measuring and Sustaining the New Economy, Software, Growth, and the Future of the U.S. Economy*, National Research Council, Washington DC. National Academy Press.

Kimberly, J. R. (1976) "Organizational Size and the Structuralist Perspective: Are view, Critique and Proposal", *Administrative Science Quarterly*, December 1976, pp. 571-97.

Kogut, B. (2003) *The Global Internet Economy*, Cambridge MA, The MIT Press

Machlup, Fritz (1972) *The Production and Distribution of Knowledge in the United States*, Plainsboro, Princeton University Press.

Masuda, Yoneji (1981) *The Information Society as Post-Industrial Society*, New York, World Future Society

Ministry of Defence of Estonia (MODE) (2008)*CyberSecurity Strategy*, Tallinn, Ministry of Defence.

Mintzberg, H. (1988) *La Estructura de las organizaciones*, Barcelona, Ariel.

Nonaka, I. y H. Takeuchi (1999) *La Organización Creadora del Conocimiento: Cómo las Compañías Japonesas Crean la Dinámica de La Innovación*, México: Oxford University Press.

Ortega, O. R. (2010) "Implementación de la Gestión del Riesgo Informático en el Proceso de Innovación Tecnológica, "Tesis de Maestría en Política y Gestión del Cambio tecnológico, CIECAS-IPN, México, mayo de 2010.

Organización para la Cooperación y el Desarrollo Económico (OECD) (2009) *OECD Communications Outlook 2009*. Paris, OCDE.

Palop, F. y J. M. Vicente (1999) *Vigilancia Tecnológica e Inteligencia Competitiva: Su Potencial para la Empresa Española*. Valencia, Fundación COTEC.

Pekka, H. (2001) *The Hacker Ethic and the Spirit of the Information Age*, New York, Random House.

Perrow, C. (1991) *Sociología de las organizaciones*, Madrid, McGraw-Hill.

Picouto, F.; Lorente, I.; García-Moran, J. P.; y Ramos., A. Á. (2007) *Hacking y Seguridad en Internet*, México, Alfaomega

Plaza, I. (2010) *Calidad en actividades de I+D+i aplicación en el sector de TIC*, México, Alfaomega.

Porter, M. E. (1987) *Ventaja Competitiva*, México, CECSA.

Robbins S. (1987) Organization theory: structure, desing and applications, Englewood Cliffs, Prentice Hall.

Smith, A. (1999) *La riqueza de las naciones*, Madrid, Alianza editorial.

Solleiro, J. L. y R. Castañón (2008) "La Inteligencia Tecnológica Competitiva como Herramienta Básica de Gestión Tecnológica," en J. L. Solleiro y R. Castañón (eds.) *Gestión Tecnológica, Conceptos y Prácticas,* México, Plaza y Valdés: 91-132.

Spafford, G. (2000) "Manual de seguridad en redes". ArCERT. Argentina. 2000. [disponible en la URL: http://www.arcert.gov.ar]

Stiglitz, J. E. (2006) "Como hacer que funcione la Globalización", Taurus, Madrid.

Thompson, J. D. (1959) *Comparative studies in administration*, Pittsburgh, Pa. Administrative Science Center, Pittsburgh University

Tilman S. (2003) "Ideologies, beliefs, and economic advice-a cognitive-evolutionary view on economic policymaking", en Pelikan, P. y G. Wegner (eds.) *The Evolutionary Analysis of Economic Policy*, Cheltenham, Edward Elgar, pp. 128-161.

Weick, K. E (1982) *Psicología social del proceso de organización*, Bogotá, Fondo Educativo Interamericano.

Woodward, J. (1980) *Industrial organization: theory and practice*, New York, Oxford University Press.