

**MILTON F. MARIN CEDEÑO
UD3248SCC7949**

**INFORMATION TECHNOLOGY: AN ANALYSIS OF THE GAP BETWEEN
SPECIALISTS AND NON-TECHNICAL STAFF AND ITS MULTI-DIMENSIONAL
IMPLICATIONS**

**A Final Thesis Presented to
The Academic Department
Of the School of Science and Engineering
In Partial Fulfillment of the Requirements
For the Degree of PhD. in Science and Engineering**

**ATLANTIC INTERNATIONAL UNIVERSITY
HONOLULU, HAWAII
MARZO, 2007**

Agradecimientos

A mi Padre Celestial por los dones y talentos que Él me ha dado que me permitieron emprender esta tarea de enriquecimiento personal.

A mi familia, a mi esposa e hijos, por el soporte emocional que siempre me han brindado y por su eterna paciencia.

A la Corporación de Operadores de Servicios Telemáticos, por la ayuda financiera y el tiempo dispensados.

A Adriana González Céspedes por su valiosa ayuda en el soporte con el procesador de palabras y su valiosa revisión a esta Tesis y sus comentarios.

A Carlos Solano Benavides por su constante apoyo en todo sentido.

A los ingenieros Róger Araya Fonseca, Michael Barquero León, Miguel Aguilar Zamora, por su excelente trabajo en la preparación de indicadores, aplicación de la encuesta, sus análisis y observaciones, sus aportes y comentarios.

Y finalmente al Dr. Franklin Valcin por su paciencia, ayuda y comentarios motivadores.

Sin el concurso de cada uno de ustedes y las bendiciones de Dios, hubiese sido muy difícil terminar con éxito este programa de Doctorado, a todos muchas gracias y que Dios les colme de bendiciones.

Resumen Ejecutivo

La desconexión es un tema prácticamente desconocido al menos bajo ese nombre. Un concepto similar es el de no alineamiento entre las Tecnologías de Información y Comunicación (TIC) y los objetivos estratégicos de una organización.

El primer concepto es más que no alineamiento, es además de esto último un problema serio de comunicación entre los profesionales tecnológicos de las TIC y los no tecnológicos o personal administrativo; un problema de dos culturas dentro de una cultura mayor que aunque a veces intentan “caminar” juntas, en ocasiones toma caminos diferentes en detrimento de los intereses últimos de una organización.

Esta tesis pretende no sólo medir el grado de desconexión existente entre los profesionales de la tecnología informática y el resto de la organización, sino que pretende dejar claro que el problema en realidad sí existe, aunque no se conozca en el fondo que se sufre o que se hayan sentido los síntomas sin preciar qué tipo de “enfermedad” se padece. Al mismo tiempo se plantea que en la medida en que la desconexión cree una brecha de diferentes proporciones, en esa misma medida la información puede estar “comprometida”, potenciar las vulnerabilidades que puedan existir y maximizar las amenazas que están presentes tanto en el ambiente externo como en el interno

Se utilizaron indicadores para medir el grado de desconexión presente en las organizaciones que permitieron que el instrumento fuera aplicado mediante una encuesta en ellas. Para efectos de establecer correlaciones e indicadores cruzados, se establecieron cinco grupos, compuestos cada uno por una serie de preguntas, las cuales se muestran en el apéndice I, que responden a los objetivos

indicados. Con los resultados obtenidos se prepararan varios gráficos para presentar en forma visual los hallazgos.

Al concluir el trabajo al menos con la información recabada, se concluyó que el fenómeno de la desconexión es tan real como la falta de alineamiento y que, definitivamente, las organizaciones deben enfrentarla con diferentes estrategias para cerrar esa brecha, que el autor cree podría de alguna manera disminuirse en forma natural, que no será suficiente si no se realizan esfuerzos en ese sentido, para cerrarla completamente.

ÍNDICE

ÍNDICE	5
I. INTRODUCCIÓN	7
EL ASEGURAMIENTO DE LA INFORMACIÓN	8
II. MARCO CONCEPTUAL Y DEFINICIÓN DE LA INVESTIGACIÓN.....	10
LOS ACTIVOS DE UNA ORGANIZACIÓN	10
EL VALOR DE LOS ACTIVOS.....	11
LOS RESPONSABLES DE LA INFORMACIÓN	13
PILARES DEL ASEGURAMIENTO DE LA INFORMACIÓN	14
LOS DESAFÍOS DEL ASEGURAMIENTO DE LA INFORMACIÓN	17
LA DESCONEXIÓN	17
RESPONSABLES DE LA INFORMACIÓN	23
LAS AMENAZAS A LA INFORMACIÓN	24
LA AMENAZA INTERNA, LOS INSIDERS	26
ESTRATEGIAS PARA HACER FRENTE A LAS AMENAZAS	31
PRINCIPIO DEL MENOR PRIVILEGIO	31
DEFENSA EN PROFUNDIDAD.....	32
PRINCIPIO DE SEPARACIÓN DE RIESGOS	33
III. DINÁMICA DE LAS EXPECTATIVAS.....	35
OBJETIVOS DE LA INVESTIGACIÓN	35
<i>Objetivo general</i>	35
<i>Objetivos específicos</i>	36
<i>Metodología</i>	36
CONFORMACIÓN DE TEMAS	38
<i>Planificación estratégica</i>	39
<i>Alineación con niveles superiores</i>	39
<i>Divulgación del PEI</i>	39
<i>Coordinación TIC – usuarios</i>	39
<i>Servicio al cliente</i>	39
IV. RESUMEN Y ANÁLISIS DE LOS RESULTADOS.....	41
ALINEAMIENTO DEL PEI CON EL PEE.....	41
ALINEAMIENTO DEL PEI CON EL PEE.....	42
UBICACIÓN JERÁRQUICA Y NIVEL DE AUDITORÍA INFORMÁTICA.....	44
ANÁLISIS Y REVISIÓN PRESUPUESTARIA	46
RELACIÓN DE PROYECTOS INFORMÁTICOS CON LA AGENDA GERENCIAL	47
ELABORACIÓN Y DIVULGACIÓN DEL PEI.....	49
SOLUCIONES INFORMÁTICAS CONJUNTAS	51
APORTE DE VALOR DE LOS SI AL NEGOCIO	53
CULTURA INFORMÁTICA.....	54
COMUNICACIÓN TIC – ADMINISTRACIÓN	56
INFORMÁTICOS Y “NO INFORMÁTICOS”	58
EVALUACIÓN SECTORIAL	60
ETAPA DE INICIO.....	63
ETAPA DE CONTAGIO	65
ETAPA DE CONTROL	66
<i>Quejas de los administradores en relación con los informáticos:</i>	68
<i>Quejas de los informáticos con respecto a los administradores:</i>	68

LA DESCONEXIÓN COMO AMENAZA	71
ESTRATEGIAS PARA DISMINUIR LA DESCONEXIÓN	77
<i>Teoría de las etapas de Nolan</i>	77
<i>La capacitación como estrategia</i>	77
<i>Cómputo de usuario final (estrategias de CUF)</i>	79
<i>Proveedores de servicios de aplicaciones</i>	79
<i>Descentralización y desconcentración</i>	80
CIERRE DE BRECHAS.....	81
DIRECCIÓN ESTRATÉGICA.....	81
V. CONCLUSIÓN	83
BIBLIOGRAFÍA	85
ENLACES EN INTERNET	86
APENDICE	87
CUESTIONARIO APLICADO	87
GLOSARIO	90

I. INTRODUCCIÓN

El concepto de seguridad siempre ha estado presente en la vida de todas las personas, aunque circunscrito a la protección de las familias y a las posesiones más cercanas a éstas, llámense propiedades muebles o inmuebles; y cuando apareció el dinero se incluyó éste también.

Con la aparición de la Internet y su exponencial crecimiento y utilización, especialmente desde los inicios de la década de los noventa, las preocupaciones básicas aumentan en forma considerable, pues aparecen otros elementos relacionados con ellas. Por eso, cabe preguntarse: ¿Está la información personal o familiar realmente asegurada y protegida? ¿Puede alguien con un “clic” del “ratón” tener acceso a información almacenada en algún banco, hospital, oficina de seguros, universidad, e incluso en la propia computadora personal? “La *Web* es una red pública, lo que significa que se intercambia información confidencial en un entorno que, por naturaleza, no es seguro.” (McCarthy:16).

Es un hecho que muchas empresas públicas y privadas mantienen información relativa a personas, a las familias de éstas y también de las organizaciones, por lo que habría que preguntarse: ¿Garantizan ellas que esa información sólo será utilizada para los propósitos propios de su quehacer y por la razón por la cual la poseen?

La gente se ha ido acostumbrando a realizar muchas transacciones “en línea”, desde mandar un “correo” personal, “chatear” utilizando los servicios de mensajería y realizar transacciones de pago, transferencias bancarias y compras, hasta obtener un título universitario a distancia, “en línea”, por medio de la Internet. Sin embargo, en la medida en que eso se haga más a menudo más regularmente también se pone en riesgo la información personal que “fluye” por la red.

No obstante que esos riesgos pueden minimizarse, para esto se requiere un enfoque diferente en cuanto al tratamiento de la información. Por ejemplo, debe ponerse mucho cuidado y atención al diseño de los sistemas y las tecnologías empleadas; deben diseñarse procesos que garanticen tanto el acceso físico a las instalaciones en las que se almacene la información, y no menos importante es que se establezcan los procedimientos adecuados para la correcta utilización, respaldo, modificación, etc. de dicha información.

El aseguramiento de la información

Antes de intentar definir qué es el aseguramiento de la información es importante hacer una acotación: “la seguridad de la información no garantiza la seguridad de su organización, de su información o de sus sistemas de cómputo.” (Maiwald:4).

Puede creerse que si se cuenta con lo que se podría entender como un entorno seguro entonces ya no hay de qué preocuparse, que si se compran los equipos adecuados, tanto de hardware como de software, al vendedor apropiado, todos los problemas en cuanto a seguridad estarán resueltos. Sin embargo, el aseguramiento de la información depende de una resolución total de una organización o de un individuo para mitigar, hasta donde sea posible, las vulnerabilidades internas y enfrentar las amenazas que haya en el entorno, con las contramedidas adecuadas.

Piénsese cuando se construían castillos. Se puede construir una puerta suficientemente fuerte como para tratar de impedir la entrada de algún extraño, pero si este utiliza un instrumento aun más poderoso que ella la derribará o destruirá en algún momento. Igual sucede si se cava un foso alrededor de una propiedad y se llena de caimanes, pirañas, etc.; pero si alguien desde adentro baja la puerta, ya la seguridad está “comprometida” o está en peligro. En este trabajo

se utiliza el término “comprometida” como parte de la jerga que es de uso común entre los profesionales de la seguridad de la información indicando que la información está en peligro de ser utilizada en forma no autorizada.

Pero, ¿qué es la seguridad de la información? Según Maywald, “son las medidas adoptadas para evitar el uso no autorizado, el mal uso, la modificación o la denegación del uso del conocimiento, hechos, datos o capacidades.” (:24).

Entonces, se puede afirmar que seguridad de la información son todas aquellas medidas preventivas que se toman para proteger tanto la información como la capacidad de los medios en que se almacena.

El aseguramiento de la información hay que considerarlo no como un evento sino como un proceso, que incluye desde aspectos infraestructurales hasta herramientas y equipo, sin dejar de lado aspectos humanos tan importantes como actitudes, puntos de vista y sentimientos; todo esto integrado en una estrategia consecuente.

Se podrían implementar mecanismos de seguridad altamente especializados, pero tener una actitud displicente o descuidada ante ellos; sin mencionar la mala fe o el sabotaje y, por tanto, obtener resultados sumamente pobres.

Para lograr un entendimiento adecuado de los pilares que integran el aseguramiento de la información es importante analizar los elementos básicos que conforman el marco de referencia, lo cual se discute en el próximo capítulo.

II. MARCO CONCEPTUAL Y DEFINICIÓN DE LA INVESTIGACIÓN

Los activos de una organización

De lo que se trata es de proteger los activos de la organización con las políticas adecuadas y dentro de marco del aseguramiento de la información, en lo cual se utilizan indistintamente este concepto y el de seguridad informática.

Los activos pueden ser tangibles o intangibles, como tradicionalmente se han clasificado. Dentro de los intangibles se incluyen ahora aspectos como la propiedad intelectual, el valor de la marca, el capital intelectual, las patentes, la información y hasta el posicionamiento alcanzado por la organización en el mercado.

Dentro de los tangibles se incluyen, entre otros, enrutadores (*routers*), conmutadores (*switches*), servidores, computadoras, impresoras, etc., y software de toda naturaleza, tanto aplicativos como operativos, sin dejar de lado los que dentro de la práctica contable se consideran como tales, o sea, todos los que se pueden convertir en dinero, ya sean líquidos o fijos.

Todos estos activos son o pueden ser potencialmente considerados objetivos para un “ataque”. Al respecto, Amanda Andrés escribe:

“Dado que Internet es una red pública, cualquier persona en ella puede “mirar” cualquier otro sistema que esté en ella. En el principio esto no era un asunto tan importante, porque la información sensible no era fácilmente accesible, pero conforme Internet crecía las compañías cada vez más frecuentemente accedían distintos tipos de información que estaba en la

red. Este acercamiento fue muy bueno para ellas pero también una gran invitación para los atacantes.” (Traducción libre) (:1).

Los activos mencionados tienen algún tipo de valor para una organización, pero hay un valor, no un activo, que a veces se deja de lado: el factor humano. Este puede ser, y definitivamente lo es, la “pieza” más importante dentro de la seguridad informática. La gente es la que logra que todas las otras partes del marco conceptual de la seguridad informática encajen adecuadamente. No importa si se cuenta con los mejores equipos de detección de intrusos, de cortafuegos (*firewalls*), de software especializado y aun de políticas y normativas adecuadas, si el personal no coopera o no tiene la actitud correcta o apropiada, o si no es el mejor personal con el que se pueda contar. En tal caso de nada sirve lo primero. El personal es el que puede llevar a la organización al logro de su visión y a potenciar el valor de toda la empresa, o bien, a ocasionar que ésta desaparezca.

El valor de los activos

Dependiendo del activo y de su importancia dentro de la organización, así también deben considerarse los riesgos y la manera en que dichos activos deben ser protegidos. En cuanto a la protección de los tangibles, se consideran generalmente adecuadas ciertas prácticas para protegerlos y, por lo normal, caen dentro del aseguramiento de la infraestructura física.

En cuanto a los intangibles, su aseguramiento ya no es tan sencillo. Algunos no se pueden encadenar o poner bajo llave, e incluso a veces no se sabe cuál es su valor. Por tanto, las preguntas que surgen son: ¿Se conoce realmente el valor de la marca?, ¿se ha medido adecuadamente el valor de las patentes? Y en cuanto a la información, ¿qué tan valiosa es?

Si se acepta el hecho de que la información tiene valor, entonces allí hay una razón para protegerla. Hay que identificar cuál es la más valiosa para la organización, en términos de terceros, llámense clientes o proveedores que mantienen alianzas con la empresa, el Estado o la misma organización, o cuánto valdría en manos de la competencia.

Como menciona Kay, “la pérdida de la lista de nuestros clientes puede ser recuperada de los respaldos que hemos hecho, si se han perdido o dañado los originales, pero si esta lista cae en manos de nuestros competidores el daño financiero potencial puede ser devastador.” (:324)

A ese respecto Andrés menciona que “las brechas de seguridad pueden tener un profundo impacto en la reputación de una empresa, en el valor de su marca o en la imagen corporativa en general.” (:3)

Hay que tener presente que los recursos de una organización no son infinitos y, por lo tanto, hay que evaluar los riesgos inherentes a cada uno de los activos para decidir cuántos de esos recursos serán asignados a su debida protección; así mismo, cuál va a ser el esfuerzo dedicado a ello. Más adelante se darán algunos lineamientos en este sentido.

Para concluir esta aparte en cuanto al valor de la información, hay que resaltar que el valor de la información puede variar en el tiempo, según las circunstancias. Lo que fue valioso en un momento, por ejemplo, mantener en secreto que la empresa pasaba por un período difícil, ya no lo será cuando se hagan públicos los informes de que la empresa ha tenido excelentes utilidades.

Dado que, según McCarthy, “la seguridad informática se basa en tres componentes las personas, los procesos y tecnología” (:32), en el apartado

siguiente se trata un aspecto fundamental, y es en cuanto a la responsabilidad que por, supuesto, tiene que ver con personas.

Los responsables de la información

Algunos de los inconvenientes relacionados con la “asignación de responsabilidades” para el aseguramiento de la información, que son fundamentales en él, han sido no sólo la poca participación de la alta dirección en aspectos relacionados con la tecnología sino también el desconocimiento que ésta tiene de los términos y de los problemas propios de la informática.

Lo anterior ha desembocado en que la alta dirección cree que el aseguramiento de la información es responsabilidad y resorte único del personal de tecnología, cuando en realidad “la gestión de seguridad y del riesgo relativo a la información debería ser un esfuerzo inspirado a nivel ejecutivo.” (McCarthy:61)

También eso lleva a pensar que el riesgo de la información es un riesgo empresarial y no tan sólo de una unidad o departamento en la organización. En este sentido McCarthy es contundente: “Los objetivos de seguridad que dependen de prioridades empresariales han de enmarcarse en un amplio conjunto de prácticas de seguridad, las cuales deben desarrollarse en colaboración con los ejecutivos, diferentes áreas de negocio, el personal de recursos humanos, el departamento de tecnologías de la información y los equipos de seguridad de la información y los equipos de seguridad de la propia empresa”. (:44)

Si todos los actores entienden bien su papel y lo ejecutan de acuerdo con las mejores prácticas y en consonancia con los procedimientos y normas de la organización, las posibilidades de que las amenazas comprometan la información de la empresa disminuyen. No se eliminan por completo dado que los ataques

pueden ser variables exógenas o endógenas, pero se puede mitigar su impacto; variables que serán discutidas más adelante.

La única manera de que la información no sea comprometida es teniéndola guardada bajo llave en una caja fuerte bajo estrictas medidas de seguridad; no conectándose a Internet o no trabajando en red; pero tales medidas estarían fuera de la realidad.

En el próximo apartado se presentan los pilares en que se basa el aseguramiento de la información, así como los elementos que permitirán la aplicación de estos elementos base.

Pilares del aseguramiento de la información

Los pilares fundamentales que constituyen los conceptos base del aseguramiento de la información son la confidencialidad, la integridad y la disponibilidad (C-I-A, por sus siglas en inglés).

Trevor Kay define dos de estos conceptos de la siguiente manera:

“Confidencialidad es el concepto que garantiza que los datos no deben estar disponibles ni revelados o publicados para conocimiento de personas no autorizadas.

Integridad es la protección de la información de daño o manipulación deliberada.”

(Traducción libre) (Kay:203)

Disponibilidad: “Que la información esté libre para ser utilizada por los usuarios autorizados cuando fuere requerida”. (Nichols:45)

Estos tres conceptos requieren algunos detalles que los clarifiquen. La confidencialidad obliga a que la información se mantenga privada o secreta y a que no sea entregada a quienes no estén debidamente autorizados para ello. Procesos como la encriptación, tanto en el nivel de datos, la infraestructura de redes y los canales de comunicación, como en los controles de acceso a las redes o a cualquier dispositivo de almacenamiento, son fundamentales para mantener dicha privacidad.

La integridad se refiere a que la información debe permanecer completa y no sufrir alteraciones cuando se utilice, a menos que existan los privilegios adecuados para hacerlo. No obstante, todos esos posibles cambios deben quedar registrados, es decir, debe llevarse una bitácora en la que se indicará quién alteró la información, cuándo lo hizo, cuáles fueron esos cambios y lo demás que el administrador de los datos considere prudente, adecuado y lógico que quede registrado. Aquella información en la cual no se pueda confiar no es o no será de utilidad; si no sirve de nada pero es confiable, puede ser que en el futuro sí lo sea; pero si no es confiable, de nada sirve. ¿Qué se ganaría con crearla y almacenarla con gasto de tiempo y dinero y otros recursos si no será de beneficio?

Nichols plantea una interesante pregunta referida a la integridad: “¿Qué información debe ser protegida de modificación ilícita o destrucción, cuánta protección se requiere y por cuánto tiempo? (:45). Estas preguntas no serán contestadas en este momento pero sus respuestas pueden ser encontradas a lo largo de esta tesis.

Por último está el pilar de la disponibilidad de la tríada C-I-A. Si la información no está disponible cuando se necesita, a pesar de su confidencialidad e integridad, entonces tampoco es de utilidad. Si los sistemas de información o las redes de computadoras no están en línea cuando se requieran, no solamente son un desperdicio de lo que se invirtió en ellas sino que podrían causar daños a

quienes dependen de ellos, pues causan pérdidas monetarias o de imagen, y hasta de reputación. Hay que plantearse en ese sentido algunas preguntas interesantes, tales como en cuánto tiempo debe estar disponible y cuánto costaría a la organización, los clientes o los proveedores el que no lo fuera.

Esos elementos de la tríada C-I-A están interrelacionados. Se puede tener un grado muy alto de confidencialidad pero la disponibilidad podría ser casi nula o nula; o bien, una muy baja confidencialidad con una alta disponibilidad. Piénsese en el catálogo de una universidad.

Cuando se ingresa a una sucursal bancaria electrónica, la integridad debe ser de muy alto nivel, lo mismo que la confidencialidad y la disponibilidad.

Cada organización, en forma particular, es la que define las características de estos pilares, dependiendo del tipo de información, y puede variar según sus propios objetivos.

Los pilares de la tríada C-I-A se fundamentan en dos “facilitadores”, la autenticación y la “no repudiación” (responsabilidad).

Kay define estos conceptos de la siguiente manera:

“No repudiación”: “es el término empleado para describir la inhabilidad de una persona de negar o repudiar el origen de la firma de un documento, o de negar o repudiar el recibo de un mensaje o documento.” (:204)

Autenticación: “es el concepto que identifica de manera inequívoca a un individuo y que garantiza su identidad. Es el simple hecho que garantiza que alguien es quien reclama ser”. (Kay:203).

La “no repudiación” provee información o evidencia de que algo realmente ha ocurrido.

La autenticación es necesaria para probar la identidad de alguien con quien se está compartiendo información. Las formas más corrientes son mediante la utilización de mecanismos de ingreso y contraseñas, tarjetas de identificación de usuarios, firmas digitales y mecanismos biométricos.

Los desafíos del aseguramiento de la información

Si la seguridad sólo consistiera en comprar algunos productos, instalar cortafuegos o un servidor *proxy*, todos en la unidad o departamento de tecnología estarían muy contentos, pero la verdad es otra. La organización debe lidiar con al menos tres grandes desafíos: las amenazas, las vulnerabilidades y los riesgos. Si se logra entender estos conceptos, es definitivo que se pueden, si no eliminar, al menos minimizar sus efectos.

Cuando se habla de amenazas debe entenderse que éstas son cualquier evento o circunstancia que puede poner en peligro los recursos de información de la entidad, desde el punto de vista de su confidencialidad, integridad o disponibilidad (C-I-A).

En el próximo apartado se aborda el tema de las amenazas, lo que permitirá establecer el objetivo de esta tesis.

La desconexión

Es un problema suscitado o derivado de un problema de comunicación. Los tecnólogos utilizan su propio lenguaje y los administradores hacen lo propio. Pero lo más grave es que por razones históricas al utilizar cada uno la jerga propia de

su disciplina, ambos mundos se fueron separando. Charles B. Wang, en su libro **Tecnovisión**, define este concepto de la siguiente manera.

“Es un conflicto penetrante y sin embargo artificial, que ha desalineado los objetivos de gerentes ejecutivos y tecnólogos, y que deteriora a las organizaciones o les impide obtener utilidades efectivas en relación con los costos de su inversión en la tecnología de la información.” (:1)

Charles B. Wang, Andreu, Ricart y Valor, y el autor de esta tesis, son los únicos que utilizan este término, y el tercero lo ha popularizado en la academia. Todos saben que en realidad hay un fenómeno que separa a estos dos tipos de ejecutivos, y aunque no han utilizado este concepto en forma explícita o quizás lo han llamado con otro nombre, nadie duda de su existencia.

Si se busca en Internet el concepto desconexión, así simple y llanamente, aparecerán poco más de un millón de enlaces. Si la búsqueda se hace más detallada, por ejemplo, mediante “desconexión informática”, pueden hallarse poco más de ciento ochenta mil enlaces. Lo interesante es que ninguno de ellos tiene que ver con el concepto de desconexión tal como lo expone Charles B. Wang. Si se explica el concepto a los profesionales de ambos mundos, informáticos y administradores, es probable que no hayan escuchado el concepto, pero sí lo han “sentido”, y todos estarán de acuerdo en que sí existe esa separación tal como se ha definido.

Sin embargo, esta tesis plantea un concepto un poco más allá de lo que dice Wang. No es un asunto solo de falta de alineamiento, es lo anterior sumado a un desconocimiento aunque sea parcial de los alcances de la tecnología por parte de los administradores y al no conocimiento completo del giro del negocio por parte de los de tecnología; se debe agregar además a la no integración de la TIC a la totalidad del negocio como elemento infraestructural.

Esta desconexión ha conllevado grandes problemas. Entre los más relevantes está el cuestionamiento de si en realidad las tecnologías de la información y las comunicaciones (TIC) han producido de acuerdo con lo que se ha invertido en ellas. En este sentido, Nicholas Carr responde con un categórico no.

Nicholas Carr primero indica: “[las tecnologías de la información] han penetrado en la industria, el comercio mayorista y minorista y los servicios empresariales; se las encuentra en las oficinas de los ejecutivos y en las fábricas, en los laboratorios de I+D y en los hogares de los clientes.”(23)

Lo anterior es cierto. Sólo basta con echar una mirada a cualquier oficina y no es necesario realizar una investigación científica para darse cuenta de que la tecnología está presente en ese lugar. Y en el caso de los hogares la utilización parcial de la tecnología, mediante el uso de computadoras personales, ha ido creciendo a un ritmo vertiginoso.

Volviendo al inicio, Nicholas Carr manifiesta que en el caso de las organizaciones lucrativas las TIC no cumplieron su promesa.(24)

Sin embargo, el asunto no se puede achacar a las TIC por sí mismas, pues no es un asunto de hardware, no es de software ni tampoco de las telecomunicaciones. Es un asunto que, en términos de seguridad informática, se llama el “efecto capa 8”, o sea, el factor humano. Para aclarar lo de la “capa 8”, el modelo OSI (*Open Systems Interconnection*) es un modelo que utiliza una estructura de siete capas para representar la transmisión de datos residentes en una computadora a una aplicación residente en otra computadora. Por ejemplo, la capa uno o capa física es utilizada para definir y controlar las señales eléctricas en un medio físico. La capa cinco o capa de sesión provee los mecanismos necesarios para que dos computadoras mantengan “una conversación” por medio de la red; y cuando se establece la sesión las dos computadoras pueden enviar información. Dada esta aclaración, en forma jocosa se habla entonces de esa

capa especial o “capa 8” que, en definitiva, puede hacer que la tecnología produzca hasta 100% o no produzca del todo. Entonces, hay que entender que el problema de la desconexión no es un asunto de tecnología y, si no se acepta eso, entonces se está lejos de resolverlo.

Las quejas de ambas partes es que hay un problema. Hay quejas de un lado que indican que los plazos de entrega de lo ofrecido por los tecnólogos no se cumplen, que se exceden en el presupuesto, etc. Por otro lado, los tecnólogos manifiestan que los administradores no los toman en cuenta en el giro total del negocio. Charles B. Wang manifiesta que “la desconexión es el único problema de la alta gerencia que no se puede delegar” y que “mientras se siga culpando a la tecnología (o a cualquier persona o cosa) seremos incapaces de combatir la desconexión.” (:26)

Las organizaciones son las responsables de que esa pared divisoria entre tecnología y administración se haya fortalecido con los años, y, aunque sea una pared de cristal, absolutamente transparente, es una pared de varios centímetros de grosor que no es fácil de derribar, dado que ellas mismas han ayudado a fortalecerla.

Muchas organizaciones crean una estructura especial, con sus normativas, procedimientos, políticas, nivel salarial, etc. diferentes para su personal del área informática. Es claro que el nivel de conocimientos que se requiere para toda esta cultura de la era de las computadoras, que son especializados, requieren una valoración distinta; pero esto no implica que se haga una diferencia tal que cree estructuras paralelas. Sin embargo, lo que más primaba era ese “terror” que muchos sentían ante esa tecnología, que hizo su aparición a mediados de la década de los cincuenta en el siglo pasado. Con la aparición de la microcomputadora se esperaba que eso fuera desapareciendo, pero no sucedió así.

Es claro que los ejecutivos utilizan su *laptop* o *desktop* para sus tareas básicas de procesamiento de documentos, preparar presentaciones o generar sus hojas de cálculo. Pero, si se produce un error, por insignificante que sea, la unidad

informática hace su aparición salvadora, puesto que el primero es “incapaz” de resolverlo por sí mismo, dado que cree que cualquier cosa que haga puede agravar el problema. El tecnólogo resuelve la situación con un halo de triunfalismo y para nada enseña al administrador cómo resolverlo si se volviera a presentar. El asunto es aun de mayor ralea cuando se trata de equipos más sofisticados, pues el administrador no desea ni verlos. Y esto es una realidad.

Los tecnólogos tienen su propio conjunto de valores, jerga, etc. con los cuales no están familiarizados el administrador o los profesionales de la gerencia. Y esta brecha se ensancha cada vez más. Los informáticos tienen su propia forma de comunicarse, los profesionales en el área de telemática la suya y, si se agregan los profesionales de seguridad de la información, se presenta una Babel de proporciones dantescas de las cuales la alta o media gerencia, sólo para citar a unos pocos, no desea ni siquiera darse por enterada.

Si se hace un poco de historia y se recuerda a los *mainframes* o grandes computadoras comerciales de inicios de los sesenta del siglo XX, se puede entender mejor este fenómeno. Eran equipos que requerían ambientes aun más controlados y asegurados que de alguna forma contribuyeron a separar físicamente a los tecnólogos de los no tecnólogos e iniciaron esta desconexión.

Los no tecnólogos abandonaron poco a poco a los tecnólogos cuando no podían entender su jerga o la manera en que programaban a esos grandes “dinosaurios” de la tecnología, o bien, no podían entender algunos de los comportamientos “extraños” de este tipo de profesional, desde la forma de vestirse -a veces un poco estrafalaria- hasta por algunos de sus hábitos y costumbres de dormir o trabajar en horas no comunes. Poco a poco se fue aislando a la función informática del resto del negocio. Entonces los objetivos del negocio se fueron desviando de los objetivos de la tecnología, y viceversa.

Es un hecho tan conocido lo anterior que se pueden encontrar en los libros de texto capítulos enteros para intentar lograr el alineamiento de los objetivos del negocio con los de la tecnología. Por ejemplo, *Aligning the IS Direction and Priorities to the Business Direction and Priorities* de Anita Cassidy, o *Strategic*

Alignment with the Business en *Managing Information Technology for Business Value* de Martin Curley, sin citar textos especializados dedicados a indicar cómo alinear los objetivos de la organización con los objetivos de tecnología, tal el caso de “Estrategia y Sistemas de Información” de Rafael Andreu, Joan Ricart y Josep Valor.

Estos mismos autores, en ese texto, hacen una breve mención a la desconexión: “Muchas empresas están todavía en una fase de descoordinación, con utilidades crecientes de la TI/SI, pero sin un proceso claro de planificación de la misma. Para empresas en esta situación, con claros síntomas de quejas por parte de los usuarios de falta de criterio en la fijación de prioridades, de **desconexión entre el departamento de TI/SI y el resto de la empresa, etc., el procedimiento...**” (Fin de la cita, el resaltado no es del original)(:4).

Más adelante indican ellos mismos: “Para aquellas empresas que han logrado derribar la pared que tradicionalmente aísla al departamento de SI del resto se abren nuevas oportunidades”. (:5)

Por lo que se ha explicado en el párrafo precedente, es un hecho que ha existido, por mucho tiempo, esa desconexión y que el esfuerzo por alinear los objetivos de las TIC con los objetivos empresariales es la prueba más fuerte de dicho fenómeno.

El propósito de esta tesis es demostrar que sí existe una desconexión tal como se explicó anteriormente. La posibilidad de que la información sea utilizada en forma no apropiada es aun mayor, o, peor aún, de que la desconexión sea una amenaza adicional y un potenciador de otras amenazas, como se explica más adelante.

En los próximos apartados, con el propósito de permitir plantear la desconexión como un problema grave para la seguridad de la información, primero se aclara quién o quiénes son los responsables de ella y quién o quiénes deberían protegerla; además, cuáles son las posibles amenazas que podrían

dañar ese valioso activo. A continuación se hace hincapié en quién o quiénes deberían ser los responsables de la información.

Responsables de la información

Algunos de los problemas relacionados con la “asignación de responsabilidades” en cuanto al aseguramiento de la información, que son fundamentales en este sentido, han sido no sólo la poca participación de la alta dirección en aspectos relacionados con la tecnología sino también el desconocimiento de ésta de los términos y de los problemas propios de la informática. Lo anterior ha desembocado en que la alta dirección crea que el aseguramiento de la información es responsabilidad y resorte único del personal de tecnología, cuando en realidad “la gestión de seguridad y del riesgo relativo a la información debería ser un esfuerzo inspirado a nivel ejecutivo.” (Trevor:43). Lo anterior lleva a pensar que el riesgo de la información es un riesgo empresarial y no tan sólo de una unidad o departamento en la organización. En este sentido Trevor es contundente: “Los objetivos de seguridad que dependen de prioridades empresariales han de enmarcarse en un amplio conjunto de prácticas de seguridad, las cuales deben desarrollarse en colaboración con los ejecutivos, diferentes áreas de negocio, el personal de recursos humanos, el departamento de tecnologías de la información y los equipos de seguridad de la información y los equipos de seguridad de la propia empresa.” (:44)

Si todos los actores entienden bien su papel y lo ejecutan de acuerdo con las mejores prácticas y, en consonancia, con los procedimientos y normas de la organización, las posibilidades de que las amenazas comprometan la información de la empresa disminuyen; no se eliminan por completo dado que los ataques pueden ser variables exógenas o endógenas, pero se puede mitigar su impacto. La única manera de que la información no sea comprometida es teniéndola guardada bajo llave en una caja fuerte bajo estrictas medidas de seguridad, o

bien sin conectarse a Internet o no trabajar en red; pero tales medidas estarían fuera de la realidad.

Se requiere saber cuál es el problema de que no haya entendimiento de los diferentes actores en cuanto a la protección de la información, y precisamente esa es la propuesta de esta tesis: la desconexión.

En el próximo apartado se tratará el tema de las amenazas.

Las amenazas a la información

Las amenazas pueden ser tanto físicas como electrónicas y dependerán del negocio al que su organización se dedique y de las diferentes relaciones de los actores que interactúen con ella.

La pregunta que debe obligatoriamente hacerse es: ¿Se debe defender a la organización de todas las amenazas posibles? Para responder, lo primero que hay que analizar son los diferentes tipos de amenazas que hay en el entorno, luego cuáles de ellas tienen una probabilidad de ocurrencia más alta y con qué recursos se cuenta para hacerles frente.

Es un hecho que los recursos económicos son escasos, que no son ilimitados e infinitos y que si se destinan a atender el asunto A se tendrán menos recursos para atender el B, o viceversa.

Por lo tanto, el conocer profundamente hacia dónde se dirige la organización, en qué negocio se encuentra, cuáles son sus objetivos y metas fundamentales, deben ser los impulsores que guíen la asignación de dichos recursos para enfrentar las amenazas.

El cuadro siguiente ilustra los diferentes tipos de amenazas

Amenazas naturales	Accidentales	Deliberadas
Terremotos	Divulgación	Alteración de datos
Inundaciones	Disturbios eléctricos	Alteración de "software"
Huracanes	Interrupción del fluido eléctrico	Amenaza de bomba
Deslizamientos		Divulgación
Tormentas de arena	Incendio	Sabotaje
Nevadas	Falla del hardware	Fraude
Tornado	Derrame de líquidos	Disturbios civiles
Tsunami	Error humano	Huelga
Erupciones volcánicas	Error de "software"	Robo
Ventiscas	Interrupción de las telecomunicaciones	Vandalismo

Fuente: Peltier. Capítulo 4. Edición electrónica. Traducción libre.

Las amenazas electrónicas están constituidas por los ataques a las redes de datos por medio de virus, bombas lógicas, caballos de troya, gusanos, y todo tipo de código malicioso.

En cuanto a las vulnerabilidades, es importante mencionar que son otro aspecto de los riesgos y se pueden conceptualizar como cualquier debilidad en un sistema o proceso que pueda ser utilizado por un atacante. El tener una vulnerabilidad en sí no comporta riesgo, excepto cuando ella hace pareo con una amenaza. Para explicar mejor esto se puede utilizar un ejemplo. Si usted vive, por

decir algo, en un lugar alejado en el estado de Oklahoma, puede dormir sin preocuparse, pues nadie intentará entrar a su casa o la probabilidad es casi inexistente. La vulnerabilidad está allí, pero no hay una amenaza, con lo cual el riesgo es mínimo. Ahora, si usted vive en una ciudad con alto nivel de criminalidad y deja la puerta abierta de su casa, ya sea de día o de noche, con las amenazas que definitivamente sí existen en su entorno, se puede decir con un alto grado de certeza que está en verdadero riesgo o que éste es muy alto.

En el caso del aseguramiento de la información, el problema es que muchas veces no se sabe que se tienen vulnerabilidades, pues estas permanecen ocultas hasta que alguien las encuentra y, la mayoría de las veces, quienes lo hacen son los que están al otro lado de la acera, los que amenazan la organización, o individuos dentro la organización, los *insiders*.

La amenaza interna, los insiders

En cuanto a las amenazas internas, definitivamente el principal riesgo puede estar en manos de los mismos colaboradores o personal interno de la organización. En inglés el término *insider* es definido como “alguien que tiene un conocimiento especial o que puede acceder información confidencial de su organización”. Ese término es muy común entre los especialistas de la seguridad informática y lamentablemente no existe un término en español que refleje el concepto. Se puede utilizar “interno”, “personal interno”, “colaborador interno”, etc., pero no es tan preciso como el de *insider*, puesto que un *insider* es cualquiera que está dentro de la organización pero no siempre será precisamente empleado de ella. Si se habla en términos de *insider threat* el asunto se vuelve un poco más complejo. Por *insider* se debe entender: “cualquiera que tenga acceso especial o conocimiento de la organización con el propósito de causar daño a ella”.

En una película cinematográfica, *The Italian Job*, se deja escuchar una frase interesante: "yo confío en todos, en quien no puedo confiar es en el diablo que tenemos dentro" (de la organización). Cualquiera de los colaboradores tiene el potencial de causar daño a una organización y no por el hecho de que reciba un salario se han comprado su corazón y su mente, y, como diría Peter Drucker, tampoco se ha comprado su completa lealtad. A veces se hace referencia a estos elementos como "la quinta columna". Peltier deja por fuera una amenaza interna, el espionaje, que es una realidad hoy en día. Para muestra un botón:

"7 de julio de 2006

No es de extrañar por tanto que, desde que en 1886 un farmacéutico creara la fórmula secreta de esta bebida, sus rivales hayan intentado encontrar la poción que tanta riqueza ha generado a sus propietarios.

Al menos de momento, el secreto mejor guardado de la centenaria compañía, está a salvo pese a la operación de espionaje industrial que ha sufrido y que ha sido abortada gracias a la ayuda de su eterna rival, Pepsi.

Tres trabajadores de Coca Cola fueron detenidos por intentar vender a Pepsi la fórmula secreta por un millón y medio de dólares pero la operación fue desbarata por el FBI.

Los detenidos son Joya Williams, de 41 años, ejecutiva de Coca Cola; Edmund Duhaney, de 43 años, e Ibrahim Dimson, de 30 años.

Coca-Cola expresó el jueves su "sincero aprecio" hacia Pepsi por su actitud, al tiempo que el portavoz de esta última firma, dijo que "hemos hecho lo que cualquier empresa responsable hubiese hecho; la competencia puede ser fiera, pero debe ser justa".

Aunque han sido varios los intentos por desvelar el secreto y el refresco se ha intentado copiar en todo el mundo, la compañía asegura que ninguna de las

fórmulas que circulan es legítima, al tiempo que se asegura que desde su origen se ha mantenido oculto un ingrediente, que tampoco en esta ocasión ha sido desvelado. Tomado de Internet: blnews.com/txt/noticia.php?id=131812 S

Con solo digitar en GOOGLE “espionaje y la fórmula de Coca Cola” se pueden hallar más de 26.000 enlaces referentes a este tema y si se digita “espionaje industrial” se pueden encontrar más de 255.000; si se busca con cuidado se hallarán historias que relatan cómo los *insiders* de todo tipo de posición en una empresa están dispuestos a “vender su alma” por unos cuantos dólares. El asunto es sólo encontrar el precio adecuado de cada uno de ellos.

Normalmente en las organizaciones se cierran los ojos ante esta verdad: la gente de adentro puede causar grandes daños. Es probable que las razones que se puedan aducir son que se puede caer en la paranoia, o bien, es mejor que nadie se dé cuenta de lo que sucedió, o que la víctima pueda volver a ser victimizada, al igual que como sucede con las personas en el mundo real. Sin embargo, como lo manifiesta Eric Cole, “el verdadero culpable es el atacante, no la víctima” (:5).

Cuando se contrata personal en raras oportunidades quienes contratan verifican aspectos fundamentales de los contratados; se aceptan las referencias tal como vienen, sin siquiera llamar e investigar sobre aspectos del comportamiento de quien se contrata; pues esto supondría un costo adicional. Este tipo de errores pueden pagarse muy caro. Ahora bien, el porcentaje de personal con bajos principios o valores no es alto, pero un solo individuo puede causar el desplome de toda una organización. Sólo hay que recordar casos muy sonados en Boeing, Emron y otras, para no ir muy lejos, que son del dominio público.

Normalmente, cuando se habla de seguridad informática en una empresa u organización las referencias irán dirigidas a los ataques externos, y en la mayoría de los casos se olvidan los ataques que pueden generarse internamente.

Muy a menudo se piden estadísticas que demuestren de dónde vienen los ataques en su mayor proporción: interna o externamente. El asunto es que eso no es de tanta importancia, ya que un ataque es un ataque. Cualquier ataque que se produzca puede causar daño a una organización, dañar su reputación o dejarla fuera del mercado, pues las consecuencias de un ataque, ya sea interno o externo, pueden ser las mismas.

El ataque interno puede causar más daño por la siguiente razón: ya está adentro. No debe saltar obstáculos perimetrales y normalmente tiene posibilidades de acceso o aun hasta privilegios para utilizar información clasificada. Si a esto se suma que la mayoría de las organizaciones han decidido facultar (“empoderar”) a sus colaboradores al darles más privilegios para utilizar información, dado que uno de los pilares del “empowerment” es precisamente compartirla con todos en la organización, el asunto se torna más complejo. En la medida en que más y más personas pueden tener acceso a información privilegiada o sensible, mayor es la posibilidad de que se produzca un daño.

Se puede argüir que se cuenta con personal altamente maduro y de sólidos principios morales. Si se está completamente seguro de eso, es probable que se minimice el riesgo; lo que no se puede garantizar es que haya una solución ideal. El autor de esta tesis ha enseñado el principio del “Síndrome de Judas” por años: “Puedes confiar en 11 de 12, aunque los haya seleccionado personalmente, (pero) si alguien se disgusta te puede vender por treinta monedas de plata o menos”.

El objeto de esta tesis no es desarrollar contramedidas para garantizar que los *insiders* no hagan mal uso de la información, pero sí indicar que se debe considerar seriamente este tipo de ataques como una amenaza real, aunque pueda ser tan sólo latente.

Se puede encontrar valiosa información sobre este tema en muchos sitios seguros de la *World Wide Web*. En la siguiente dirección <http://www.sei.cmu.edu/publications/documents/04.reports/04tr021/04tr021.html>

del Engineering Institute/Carnegie Mellon se encontró lo que se describe a continuación:

“La motivación de 81% de los “insiders” fue el dinero. 27% de los “insiders” tenían problemas financieros al momento del incidente. Además de los motivaciones financieras, 23% fueron motivados por la venganza, un 15% estaban insatisfecho con la administración, la cultura o las políticas de la organización; 15% buscaban respeto, y había 27% con otros motivos” (Traducción libre del autor de este estudio).

El artículo es de gran interés y se invita al lector a revisarlo profusa y completamente.

Es interesante resaltar que en 78% de los incidentes mencionados en el reporte los *insiders* éstos eran usuarios autorizados con cuentas activas en los sistemas informáticos en el momento del incidente. En 43% de los casos los *insiders* usaron sus propios nombres de usuario y sus contraseñas para provocar el incidente. Esto indica que no rompieron o quebraron la seguridad de los sistemas sino que tomaron absoluta ventaja de sus privilegios. En algunos casos ni siquiera se preocuparon por hacerlo en forma anónima, lo cual puede significar que, o desconocían que podían ser capturados, o estaban “bastanteando” el campo. Para concluir, 26% de los casos citados en el estudio utilizaron las cuentas de sus colegas o equipos que estaban “abiertos”, esto es, se dejaron no atendidos con sus sesiones abiertas. Con lo anterior se desea demostrar que un problema fundamental en la seguridad es definitivamente el factor humano, “la capa 8”.

Con el propósito de dejar allanado el camino para el planteamiento de los indicadores de desconexión y su relación con las amenazas, se proponen a continuación algunas estrategias para lograr mitigar los riesgos a que está sometida la información.

Estrategias para hacer frente a las amenazas

Las estrategias en este caso deben obedecer a principios fundamentales puesto que las estrategias son las que permiten, por medio de tácticas o actuaciones concretas, la implementación de las medidas del plan de seguridad.

Principio del menor privilegio

Este principio dicta que sólo se debiera permitir el mínimo acceso que se requiere por parte de alguien para alcanzar su objetivo.

Como lo indica Nicholls, “el universo de información puede ser subdividido de manera tal que los individuos sólo reciban acceso al conjunto de información que necesitan para lograr ejecutar su tarea, pero no a la información que no necesitan.”(:28)

Eso implica que el acceso a un recurso sólo debiera permitirse a personas específicas o a procesos que así lo requieran. Además, que solo tuvieran acceso a la porción de información necesaria para completar una tarea. Y, por supuesto, sólo por el período requerido.

La aplicación de una política de este tipo, que tiene una razón de ser fundamental, puesto que no es necesario que alguien de recursos humanos accese información del departamento de informática no relacionada con asuntos de personal. La dificultad estriba en tener que identificar cada documento o párrafo, e incluso frase, que pueda ser accesada por tal o cual individuo, o que no pueda hacerlo. Por otro lado, este principio permite que muchas decisiones en cuanto al manejo de la información sean más sencillas y, por ende, más seguras.

Para aclarar la última frase es necesario indicar lo siguiente. Controlar el uso de la información y, en especial, la que es de valor o bien clasificada se puede

alcanzar bajo este principio del menor privilegio. Se procura que la información no caiga en manos de quienes no deban tenerla. Ya se resaltó que los ataques pueden venir de dentro de la organización. En este sentido, Andrés menciona: “Las personas son el componente de seguridad más importante. A menudo también son el enlace más débil en una infraestructura de seguridad.” (Cap.1, pág. 4, versión electrónica).

Además, al limitar el privilegio de acceso a la información se puede prevenir que un atacante pueda llegar fácilmente a ella. Si no se posee una política restrictiva, la información podría estar comprometida y dicho atacante podría tomar toda la información. Este principio también permite llevar un control de quiénes accesan la información que ha sido clasificada o restringida.

Este principio no sólo se aplica a los sistemas de información basados en computadoras. Se puede restringir el acceso físico a información privilegiada que no reside precisamente en componentes computarizados. Y también se puede restringir el acceso a lugares dentro de la organización, independientemente de la información que posea. Puede restringirse el acceso a equipos que son parte de la estructura de redes de la organización, por ejemplo, enrutadores, conmutadores o cortafuegos, y así mismo a impresoras o a cualquier otro equipo que no deba ser manipulado por terceros, que nada tiene que ver con los procesos propios del sistema.

Defensa en profundidad

Este principio es fundamental e indica que no se puede basar la defensa de la información en un solo mecanismo de seguridad; es aconsejable hacerlo por capas o niveles. Ante la eventual falla de uno de los mecanismos entran en acción los contingentes.

Si el foso no fue suficiente para impedir el intento de ingresar al castillo, entonces entran en acción los calderos de aceite hirviendo; si esto no impide el avance, las piedras o, finalmente, las flechas y lanzas, pueden lograrlo. Si todo

esto falla, no quedará más remedio que el enfrentamiento cuerpo a cuerpo. Hay que recordar que aun la defensa bien planificada puede ser violada desde adentro, por la famosa quinta columna.

Si un atacante está dispuesto a entrar es probable que lo consiga. Todo dependerá de: los recursos que posea, el tiempo y la disposición de lograrlo. La historia de las grandes batallas documenta en forma amplia cómo pequeñas vulnerabilidades o el exceso de confianza acabaron con la defensa mejor planificada.

En definitiva, una estrategia bien pensada bajo este principio puede constituir una barrera formidable en contra de los atacantes. Bajo este mismo principio lamentablemente se aplica aquello de que si el vecino es más vulnerable es probable que el atacante vuelva su vista hacia él.

Principio de separación de riesgos

Ya en otro apartado se comentó lo que es un riesgo. Hay que recordar que los riesgos son parte inherente al hecho de estar en este mundo. Los riesgos son la antítesis de la seguridad y, por ende, hay un deseo de eliminarlos. Esto no es posible y nadie lo ha logrado. Se podría intentar, mediante un análisis meticuloso y un plan bien elaborado, eliminarlos en la medida de lo posible. Sin embargo, el problema mayor podría ser el costo, comparado con las posibles pérdidas que los riesgos podrían causar.

Se puede pensar en un sencillo problema, la posibilidad de que el auto pueda quedarse sin acumulador. Es un riesgo latente. Entonces, como medida para mitigar esa posibilidad, puede tenerse un acumulador de repuesto. Ahora bien, ¿cuál es la posibilidad de que el acumulador se agote y lo haga en los peores momentos? De suceder, ¿no existen otras posibilidades para solucionar el problema?, por ejemplo, llamar al servicio de emergencias y conseguir una unidad de repuesto; o bien, si el automóvil no es automático, darle velocidad al auto y obligar al generador a dar ignición al motor. Se puede tener un acumulador de repuesto, pero si la unidad base no falla es probable que la vida útil de la unidad

de repuesto se agote al mismo tiempo que la primera. Se incurrió en un gasto sin sentido. Pueden darse otros ejemplos más sofisticados, los cuales se dejan al ingenio del lector.

Los riesgos pueden separarse en riesgos empresariales, de redes, de servidores o de *host*, o de aplicaciones. Dentro de los riesgos empresariales pueden citarse los de tipo técnico, de carácter financiero, ambientales, etc. En cuanto a los de redes, son aquellos que pueden dejar inútil la infraestructura, ya sea por aspectos físicos o por ataques de denegación de servicios (un tipo de ataque que podría deberse a que se hacen tantas solicitudes al servidor que este colapsa); o porque un atacante logra el control de él. Los riesgos a que puede estar expuesto un servidor son, por ejemplo, que permita el acceso no autorizado al equipo. Los relativos a las aplicaciones es todo aquello que pudiera dejar en riesgo la información o comprometida, a partir de la utilización programas de software especializado o de otros programas aplicables.

Una vez analizados los diferentes tipos de riesgos queda claro que todos están interrelacionados. Dependiendo del tipo de riesgo y del impacto que éstos pueden tener en el valor de la información así serán las medidas que deban tomarse para mitigarlos.

En el próximo capítulo se plantea lo que se espera del objeto de esta tesis.

III. DINÁMICA DE LAS EXPECTATIVAS

En la actualidad, dentro del ambiente empresarial es sumamente conocida la separación que existe, tanto en el nivel operativo como en el estratégico del área de sistemas de información o de las tecnologías de la información y comunicación (TIC), con el resto de la organización. Aunque no se utilice el nombre de desconexión, con estudios preliminares y la aplicación de breves cuestionarios se ha podido comprobar que en realidad sí existe dicha problemática. Todos aceptan que hay problemas de alineamiento entre los objetivos de TIC y los de la organización o empresa. Pero la desconexión es más que una falta de alineamiento.

La hipótesis propuesta lleva dos grandes orientaciones: la de demostrar que en realidad sí existe una desconexión y la de dejar planteado que dicha desconexión se constituye en una verdadera amenaza o, al menos, en la potenciadora de las amenazas descritas en el capítulo dos, en el que se define el concepto de investigación.

Se plantean una serie de preguntas en un cuestionario, que se constituyen en los indicadores de desconexión.

Objetivos de la investigación

Objetivo general

Medir el grado de desconexión entre las TIC y el resto de la empresa, con el propósito de valorar su relación con las amenazas internas y externas a las que está expuesta la información de una organización humana.

Objetivos específicos

- Evaluar el grado de desconexión que hay en los diferentes sectores encuestados.
- Analizar la visión que tiene el usuario administrativo del área de tecnologías de información y comunicación.
- Analizar cómo ven los informáticos su papel dentro de la administración
- Determinar si existen o no planes informáticos alineados con los planes de la organización

Debido a que el siglo XXI se perfila como un periodo en el que el desarrollo humano estará basado en la informática, es necesario emprender esfuerzos para acercar al cada día más creciente departamento de tecnologías de la información y la comunicación (TIC) con el resto de la empresa, para intentar cerrar la brecha que en la actualidad está presente en la mayoría de compañías alrededor del mundo.

En el apéndice de este estudio se incluye un listado de todos los indicadores que se utilizaron con el fin de medir el nivel de “desconexión” entre TIC y el negocio, para poder de esta manera dimensionar de alguna manera el efecto mencionado.

Metodología

Ya que las organizaciones son reacias a admitir que existe un problema en ellas, la metodología empleada para conseguir que se contestara el cuestionario no siguió ningún lineamiento probabilístico, por cual su validez puede ser cuestionada en tanto no se ajustó al método científico. Fue aplicado de manera profesional a aquellas personas de un total de cuarenta instituciones que estuvieran dispuestas a contestarlo. A todas ellas se les garantizó que la

información iba a ser procesada de manera sectorial y que no se identificaría a su organización, empresa o institución de manera específica.

La encuesta se aplicó en la misma semana y de manera directa. Fue realizada por tres estudiantes de un programa de maestría en administración de la tecnología de una universidad privada, quienes ayudaron a procesar y tabular la información, y también participaron directamente en el procesamiento de ella con sus comentarios, análisis y observaciones, e incluso con sus propias conclusiones, las cuales se tomaron en cuenta para redactar la interpretación de los resultados del capítulo IV.

Adicionalmente, se aplicó el mismo cuestionario para ponderar las 15 respuestas. Participaron en el trabajo quince estudiantes del mismo programa en dicha universidad, además de 10 colaboradores más. Con ese segundo trabajo se diseñó un indicador de desconexión total.

Es un hecho comprobado que los procesos de negocios en las empresas de este mundo globalizado dependen en gran medida de las tecnologías de la información para operar, pero, como ya se ha planteado, existe un nivel de desconexión de tecnologías de información con el resto de la empresa.

Las tecnologías de información y comunicación (TIC) y las áreas de negocio de la empresa a menudo tienen objetivos que no están alineados. TIC focaliza sus esfuerzos en la reducción de costos de mantenimiento y funcionamiento de sistemas, mientras que el negocio necesita que TIC maximice la creación de valor. Cuando existe desconexión de TIC con el negocio es común observar que los ejecutivos de TIC se definen como “proactivos”, mientras que los ejecutivos en las unidades del negocio observan a sus colegas de TIC como “reactivos”.

En el caso contrario a la desconexión de TIC con el negocio, está claro que esta área impulsa a la organización y maximiza los beneficios; dicho de otro modo, genera valor.

Tradicionalmente la función de TIC fue considerada como un área separada del negocio, responsable de proveer servicios básicos como son: servicios de red y desarrollo de sistemas. Hoy se puede decir, sin lugar a dudas, que las tecnologías de la información y la comunicación son fundamentales para la gestión de los recursos de la empresa. Son indispensables para la gestión de la relación con los clientes “CRM” y claves para la gestión del conocimiento del negocio y para el crecimiento e innovación continua.

En la actualidad la vinculación entre el cuadro de mando integral (CMI, conocido por sus siglas en inglés como BSC) y el negocio constituye un método fuerte para alinear las TIC con toda la empresa. La relación entre los objetivos del negocio con sus métricas, y la relación de los procesos de TIC con sus objetivos y métricas, es de gran importancia para disminuir la desconexión de las TIC con el negocio.

Finalmente, muchos responsables de TIC están utilizando el modelo de CMI para acelerar su proceso de generación de valor, y convirtiéndose en socios de la estrategia del negocio, sin perder de vista el desempeño requerido en el uso de los recursos.

Conformación de temas

Para efectos de establecer correlaciones e indicadores cruzados, se establecieron cinco grupos, compuestos cada uno por una serie de preguntas, las cuales se muestran en el apéndice I, que responden a los objetivos indicados. Los grupos fueron los siguientes:

Planificación estratégica

En este apartado se agruparon una serie de preguntas dirigidas a la elaboración, divulgación y actualización del plan estratégico informático (PEI), con fines de determinar la participación colaborativa de la empresa en su desarrollo y, por ende, establecer conexión o desconexión mediante este instrumento.

Alineación con niveles superiores

Con este tema se conoció la ubicación del gerente con respecto a las TIC en términos de su organización, lo cual incide positiva o negativamente en la conexión o desconexión entre TIC y el resto de la organización.

Divulgación del PEI

Se midió el nivel de conocimiento del PEI por parte de la organización, en términos de su divulgación y la participación de los diferentes niveles en su construcción y seguimiento.

Coordinación TIC – usuarios

Este es un factor importante en materia de conocer grados de conexión o desconexión. El liderazgo de los patrocinadores, especialmente en el desarrollo de proyectos, es fundamental para su conexión con las TIC y para el aporte que estas soluciones brinden a la organización.

Servicio al cliente

El servicio al cliente mide en mucho si hay desconexión o no, por medio de la capacitación que se les haya suministrado, el lenguaje en que se comuniquen tecnólogos informáticos y administradores, la claridad con que se solicita y presta el servicio, así como la prioridad con que se atiende.

Una vez abordado este marco conceptual fundamental para el planteamiento adecuado de la investigación se procederá ahora a presentar los hallazgos de la investigación, mediante la metodología utilizada. Se presentan gráficos que resumen las encuestas realizadas, por sector, con breves explicaciones de cada uno, aunque los cuadros se diseñaron para que fueran lo más explicativos posible.

IV. RESUMEN Y ANÁLISIS DE LOS RESULTADOS

Alineamiento del PEI con el PEE

El alineamiento del plan estratégico informático (PEI) con el plan estratégico de la empresa (PEE) puede lograrse de dos maneras, en forma pasiva o en forma activa. La forma pasiva consiste en definir el PEI a partir de la estrategia corporativa y las necesidades concretas de cada unidad de negocio.

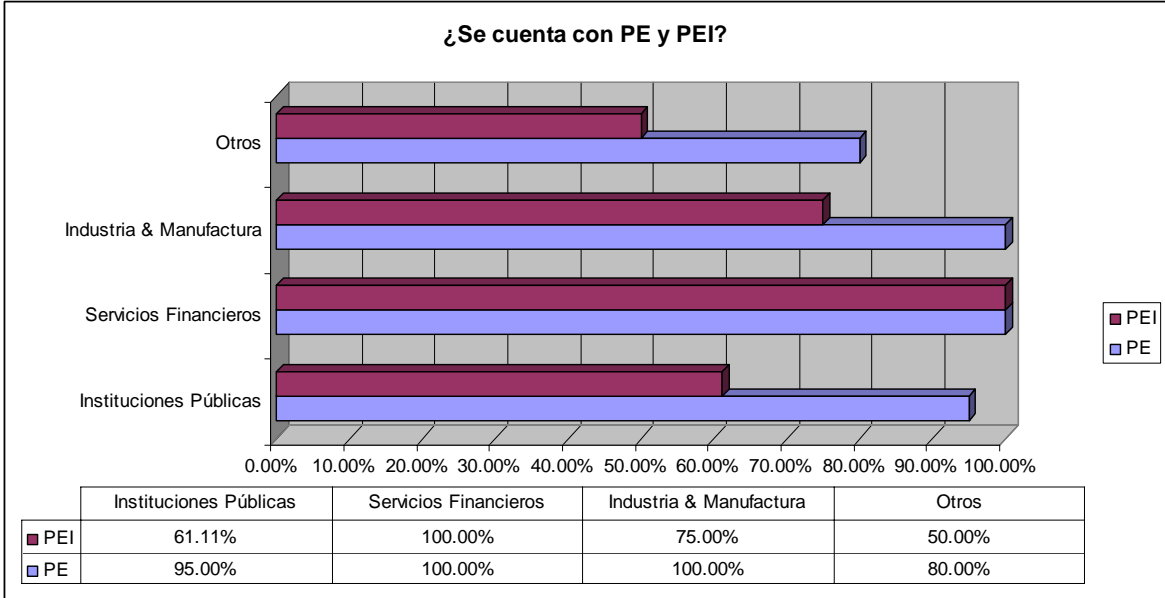
Esa metodología es adecuada “cuando si bien las TIC constituyen un soporte importante para la estrategia del negocio, no son en sí mismas una fuente de ventaja competitiva ni tienen el potencial de convertirse en una pieza fundamental de la estrategia competitiva a mediano plazo”. (Sandra Sieber y otros: 34) La metodología pasiva aparece cuando en una organización se dispone de muy pocos sistemas de información, están disgregados y la unidad de TIC soluciona los problemas conforme se hacen presentes.

En forma activa implica que el PEI se desarrolla en paralelo con el desarrollo del PEE, e indica que la unidad de TIC participó junto con el personal de la empresa mientras se desarrollaba el PEE. Esto permite que se alcance un mayor entendimiento de las necesidades del negocio en materia de tecnología como respaldo fundamental de todos sus procesos. En ambos casos la participación de la alta gerencia es fundamental.

Del análisis del gráfico 1 se deduce que, según las empresas encuestadas del sector público, 95% tienen un plan estratégico “empresarial” y menos de 62% cuentan con un plan estratégico informático. Lo sorprendente es el sector financiero analizado, que cuenta tanto con un PEE y con un PEI en su totalidad. Esto puede verse incluso como normal, dada la competencia que se desarrolla en ese sector, además de las regulaciones y lineamientos de la Superintendencia General de Entidades Financieras (SUGEF), que obliga a que estos planes se

desarrollen. Con esta información no se puede deducir si los planes están alineados o no. Los próximos gráficos aclaran si existe alineamiento o no.

Gráfico 1



Fuente: Elaboración propia para la investigación

Alineamiento del PEI con el PEE

En el cuestionario se incluyeron preguntas que permitieron medir el grado de alineación del PEI con el PEE de los diferentes sectores considerados. En el gráfico 2 se refleja una participación muy baja del área de TIC en la elaboración del PEE. Ante la pregunta de si la unidad de TIC participa en la elaboración del PEE, en el caso de las instituciones financieras las respuestas fueron positivas en 85%. Si se vuelve al gráfico anterior se puede observar que este tipo de instituciones tienen PEI y PEE en su totalidad. Esto indicaría al menos que hay una falta de alineamiento de 15%, aunque el hecho de que haya 85% que manifestaron que sí participaron tampoco es indicativo de que cuando se elaboró el PEI éste se hizo en plena concordancia con el PEE.

Si bien es cierto el PEI no debe desarrollarlo el gerente de TIC, o sus colaboradores, también lo es que si no participaron en el desarrollo del PEE difícilmente van a determinar si el PEI está o no alineado con el PEE. Los otros sectores muestran la misma tendencia de poca participación. La pregunta siguiente sí es un indicador de que hay falta de alineamiento. Al consultarse si el PEI está alineado con el PEE, en el caso del sector público, manifestaron que está alineado sólo en 83,64%. Hay que notar que en dicho sector solo 61% cuentan con un PEI; por lo tanto, sí existe una desconexión, pues hay una relación directa entre la falta de PEI y la falta de alineamiento.

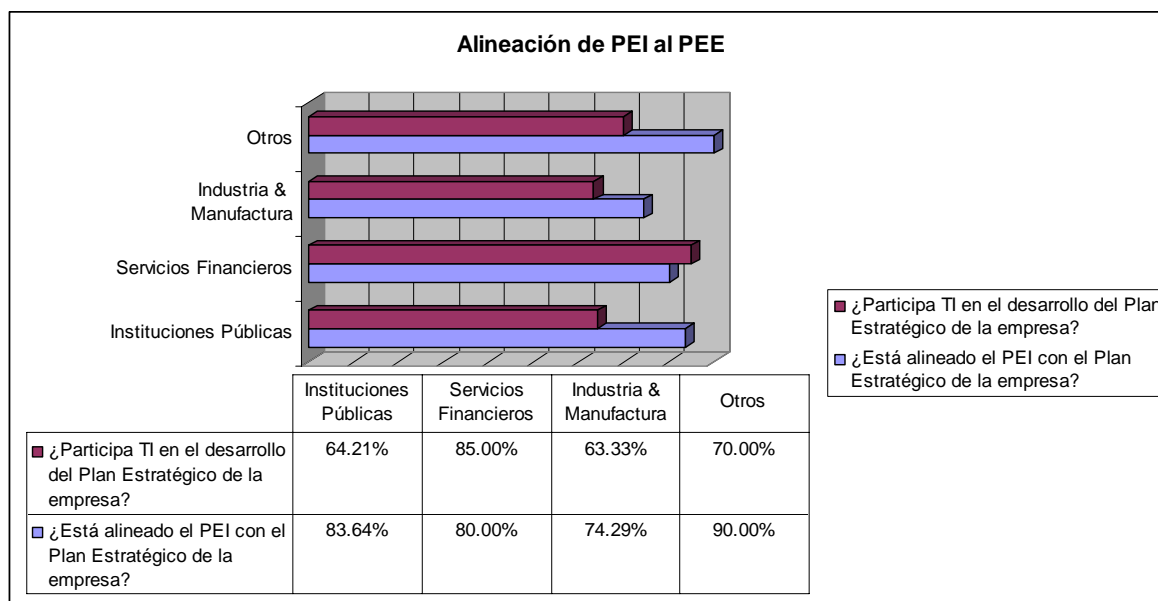
En el sector financiero, que cuenta con 100% de PEI y PEE, existe una falta de alineamiento de 20%. Independientemente del nivel de desconexión, es un problema que debiera ser analizado cuidadosamente por esas instancias, dado que en este sector la intensidad de la rivalidad es muy alta, las fusiones están a la orden del día y el ingreso e interés de fuertes grupos financieros bancarios son notorios.

En el mes de octubre del 2006 el Scotiabank de Canadá adquirió el Banco Interfin, el banco privado nacional costarricense con los mayores activos y gran solidez e imagen. También cambió de dueños un tiempo antes el Banco Banex, adquirido por un grupo panameño, que a su vez fue adquirido, en el 2006, por un banco de Hong Kong. Independientemente de lo anterior, en la industria financiera los factores claves del negocio son credibilidad y confianza, índice de intermediación, índice de morosidad y servicio basado en una fuerte plataforma tecnológica. Entonces, la falta de alineamiento entre el PEI y el PEE es o puede ser un problema grave, puesto que el que una empresa o institución no esté desarrollando competencias en sus factores claves de negocio les puede dejar fuera, con el agravante de que pueden arrastrar a todo el sector a problemas insospechados.

Es interesante notar que el sector “otros” manifiesta que el grado de alineamiento es de 90%. En este grupo se incluyeron varias universidades estatales y privadas, además de líneas aéreas. Aunque por limitaciones del estudio no se presentan los datos en forma separada, sí se observó que en las

universidades se da un alineamiento casi de 100%, lo cual es lógico que se presente en la academia. En las líneas aéreas fue de 100% y al efectuar la investigación se pudo constatar que existe un verdadero alineamiento, pues cuentan con instrumentos adecuados, como el cuadro de mando integral y otro tipo de metodologías con indicadores adecuados, que garanticen que las estrategias tecnológicas responden a las estrategias del negocio.

Gráfico 2



Fuente: Elaboración propia para la investigación

Ubicación jerárquica y nivel de auditoría informática

En la década de los setenta el profesor de Harvard Richard Nolan presentó una teoría que se conoce con el nombre de teoría de las etapas de Nolan, la cual se tratará en el capítulo de análisis general, pues aporta información que puede ser relevante para entender aspectos de la desconexión.

En el sector de la industria y la manufactura la ubicación del gerente de TIC en un muy alto porcentaje (87,5%) no está adscrita al máximo jerarca, lo cual le

dificulta una mejor relación para posicionar las TIC como parte de la cadena de valor y para desarrollarla en función del negocio; y una situación similar se da en las instituciones públicas (50%). Este es un factor que coadyuva en la desconexión. De acuerdo con la teoría de las etapas de Nolan, estas instituciones estarían en la etapa de contagio, pues es en esta etapa en la que el departamento de sistemas de información es promovido y pasa a depender de la gerencia de finanzas o de la contraloría, pero no de niveles superiores, como la gerencia general. Si en instituciones que se consideran maduras o con relativa permanencia en el mercado el departamento de sistemas aún se encuentra dependiendo de los niveles administrativos inferiores, y esto puede ser reflejo del grado de desconexión que existe en la organización.

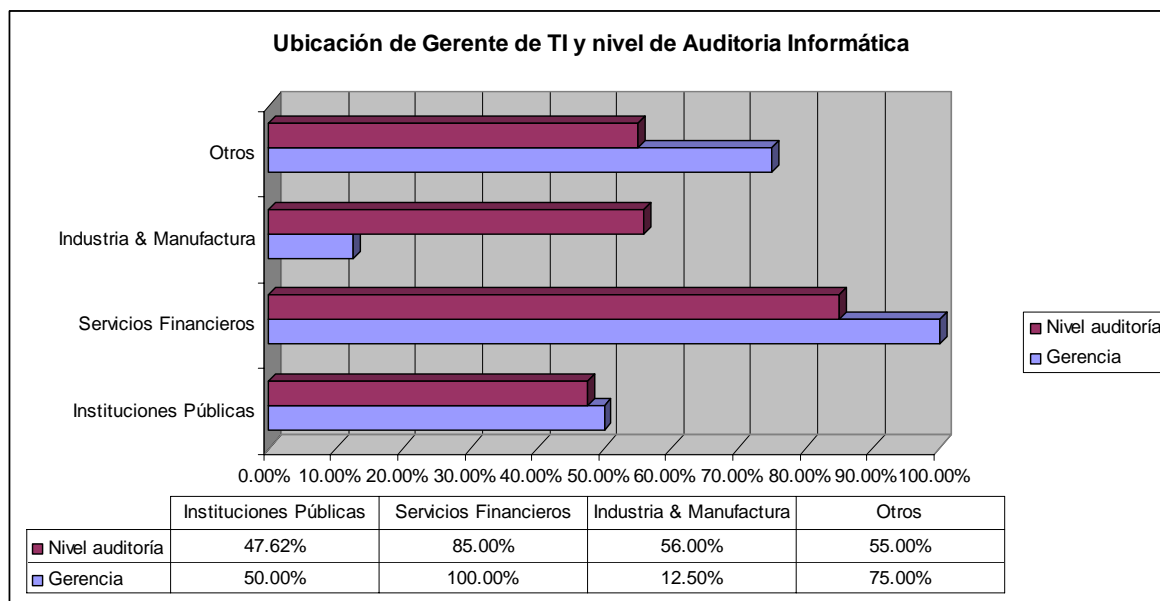
En las instituciones de corte financiero 100% de los directores de TIC reportan a la alta dirección; pero, como se verá adelante, tampoco es indicativo de que la alta dirección esté “alineada” con la tecnología. De hecho, 10% de instituciones que no tienen un lugar en la agenda para asuntos de tecnología. Entonces, si 100% de las instituciones financieras tienen un PEI, hay un alineamiento de 80%, y 100% si reportan a altos niveles y no están presentes en la agenda gerencial. Entonces existe, aunque en menor grado con respecto a los otros sectores, una desconexión entre ambos mundos.

Es mucho más grave, y así se preveía, y fue la razón de plantearse esta hipótesis para esta tesis de grado, que en los otros sectores la desconexión sería mayor.

Excepto para el sector financiero, la auditoría de sistemas apenas si alcanza 56%, en el mejor de los casos. Este tipo de procesos es fundamental que se realicen constantemente en las empresas, dado que el activo más valioso en las organizaciones es la información, y, como ya se ha mencionado en los primeros dos capítulos, es responsabilidad de todos que dicha información esté salvaguardada de mal uso. La desconexión se “alimenta” de la falta de auditorías y, lo que es más grave, como se verá más adelante, puede propiciar que se

generen vulnerabilidades y que las organizaciones sufran ataques que pongan en peligro sus sistemas.

Gráfico 3



Fuente: Elaboración propia para la investigación

Análisis y revisión presupuestaria

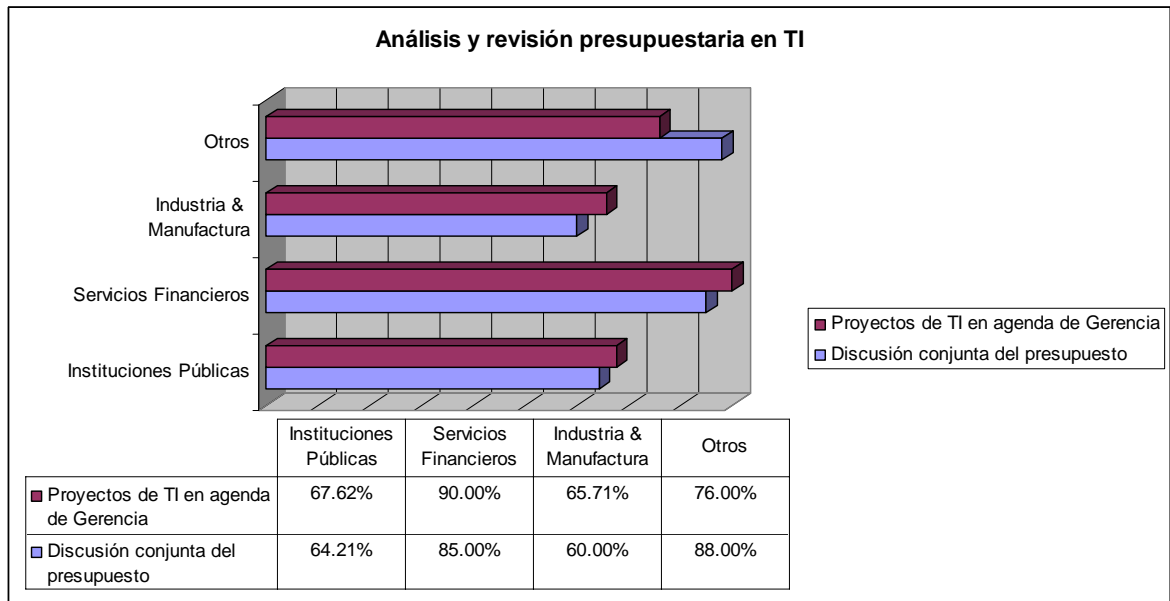
Es normal escuchar a gerentes de TIC decir que sus presupuestos fueron recortados sin consultarles o que no fueron aprobadas todas sus peticiones. Generalmente esto sucede por la falta de presencia de TIC en la agenda de la organización.

En el gráfico 4 queda evidenciado que al no existir el tema de TIC en la agenda de los gerentes, especialmente el máximo jerarca, el presupuesto en tecnologías de información puede pasar a ser algo irrelevante. Es claro que en la

administración pública (64,21%) y en el área de manufactura (60%) el presupuesto de TIC no es motivo de análisis en la organización; posiblemente su composición es para efectos de gasto, sin agregar valor al negocio.

El caso contrario se da en el sector financiero, en el que la tecnología, como factor clave del negocio que es, es nervio y motor de la organización. Sin embargo, si se recuerda, en las instituciones bancarias existe un alineamiento de 100% entre PEI y el PEE.

Gráfico 4



Fuente: Elaboración propia para la investigación

Relación de proyectos informáticos con la agenda gerencial

Si se parte de que las TIC son parte de la agenda de trabajo del máximo jerarca, entonces éste se convierte en una fuerza impulsora que facilite la puesta en marcha de tecnología que aporte al negocio.

Cuando se cuenta con un comité gerencial de informática (CGI), representado por los diferentes niveles superiores de la organización, esto viene a constituirse en fuerzas de apoyo a la puesta en marcha de TIC en ella.

Otro aspecto por considerar es que si se tiene auditoría de sistemas ésta generará informes que serán del conocimiento de la alta dirección si TIC forman parte de la agenda de trabajo de estos últimos. Obviamente, ésta es una fuente de información muy valiosa para que ese nivel esté debidamente informado sobre posibles desviaciones del PEI con respecto al PEE.

En el gráfico 5 se nota claramente que, excepto el sector financiero (85%), los otros sectores están muy débiles en relación con las auditorías de sistemas. Situación similar se da con la incorporación en la agenda de trabajo del jerarca de temas relacionados con TIC (instituciones públicas, 67,62), y en manufactura e industria 65,71%. Los comités de informática están muy incipientes en otros sectores (40%).

Se desprende de esto que, salvo el sector financiero, la “no integración” del máximo jerarca con un comité de informática, y con la fiscalización de las actividades de TIC, muestra una gran desconexión en esta materia en los sectores de instituciones públicas, industria y manufactura.

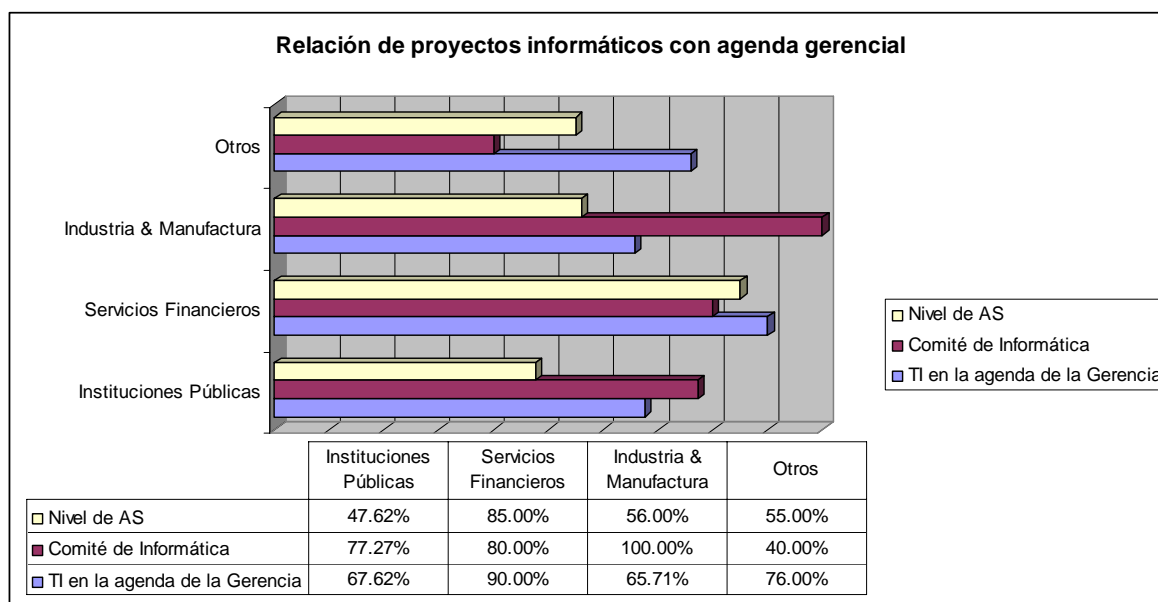
Si se efectúa un análisis más detallado pueden observarse “disonancias”. Por ejemplo, en el sector manufactura se cuenta con un comité de informática en 100% de los casos. Sin embargo, los temas relacionados con informática sólo están presentes en menos de 66%. Habría que preguntarse por qué se da esta situación. Si el comité está bien integrado se debe contar con personal de muy alto nivel gerencial que efectúe el enlace entre TIC y la alta dirección, pero parece que esto no sucede.

Si se recuerda el gráfico 2, hay problemas de alineamiento entre el PEI y el PEE, además de que TIC no participa en la formulación del PEE. Por lo tanto, aunque no se cuenta con más información puede ser que el comité responda sólo a “una moda”, o no haya tenido la fuerza suficiente para “pesar” en la alta administración. Esto definitivamente apunta, tal como se ha planteado, a un problema alto de desconexión.

Es interesante resaltar también que, aunque la situación en el sector financiero es mucho mejor que en los otros, hay una diferencia sustancial; 20% no

cuentan con comité de informática, aunque hay un alineamiento de planes entre TIC y la administración. Si están alineados lo normal es que existan comités en 100% de los casos, cosa que no sucede según los datos de esta investigación. A pesar de que no hay 100% de temas de tecnología presentes en la agenda de la administración, el porcentaje es alto, aun cuando no hay 100% de comités. ¿Hay o no hay desconexión? De acuerdo con las premisas que se han ido planteando a lo largo de esta tesis, existe una leve desconexión.

Gráfico 5



Fuente: Elaboración propia para la investigación.

Elaboración y divulgación del PEI

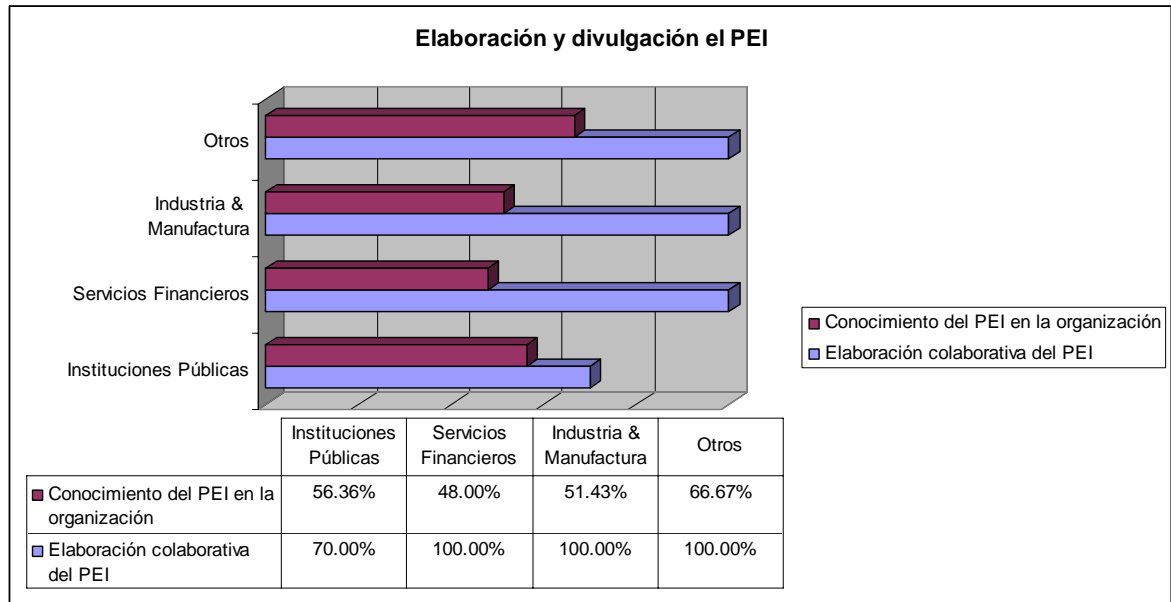
Hay varias estrategias para eliminar la desconexión, que no es más que un problema de comunicación. Por el momento se mencionan dos que pueden ayudar a disminuir este fenómeno: la divulgación del PEI y el desarrollo participativo de ésta. Si se tiene un PEI y no se divulga se puede tener menor apoyo de los diferentes niveles de la organización, al no conocerlo.

Por otro lado, si no hay participación de todas las partes involucradas en las TIC, igual se pueden tener diferentes grados de desconexión y lógicamente un plan incompleto. Sin embargo, la investigación arrojó un dato interesante: la participación es altísima en todos los sectores y la divulgación muy baja. Eso significa que no ha permeado el PEI en los niveles inferiores, y genera desconexión en los niveles operativos.

Una de las mayores fallas en todos los sectores es la divulgación del PEI, lo cual repercute en que haya un alto grado de desconexión en las entidades. El porcentaje de conocimiento es bajísimo, pues oscila entre 48% y 66,67%. Se podría pensar que no interesa divulgar los planes por razones de competencia, pero sí se divulga normalmente el PEE. Puesto que el PEI es muy técnico, no existe una razón de peso para no hacerlo, excepto en el caso del sector financiero, pues debe recordarse que la tecnología es un factor clave del negocio en ese tipo de industria. Podría pensarse que ésta sea la razón, pero habría que investigar por qué sucede eso, y fue algo que no se abordó en el momento de aplicar esta encuesta.

Hay que resaltar que, excepto en el sector público, según las respuestas de los encuestados hay una participación de 100%. Sin embargo, este resultado responde al análisis sectorial agrupado, puesto que los informáticos dicen que sí participaron los administrativos, mientras que estos últimos manifestaron que no lo hicieron. Esto refleja que no todos los actores participaron de la manera adecuada en el desarrollo del plan y que algunos “resienten” su “no participación”, y que suponen que debieron haberlo hecho. Este tipo de elementos son los que hacen de nuevo sostener la hipótesis de que aún existe desconexión en los sectores en donde hay un acercamiento entre TIC y la administración.

Gráfico 6



Fuente: Elaboración propia para la investigación

Soluciones informáticas conjuntas

En el gráfico 7 se puede observar con mayor claridad que existe desconexión. Este fenómeno se hace muy evidente cuando el desarrollo de sistemas se realiza sin la debida participación de los usuarios. Ha sido tema de controversia constante en el mundo de la tecnología la poca participación de los usuarios en este proceso. Esto puede ser entendible por los problemas de comunicación suscitados por la jerga de los tecnólogos.

También en este gráfico se muestra muy claramente que en las instituciones públicas el desarrollo de proyectos de TIC en forma conjunta no alcanza 54% y podría reflejar un nivel de poca importancia para los jercas de estas instituciones. Al medir el liderazgo y la evaluación de proyectos por parte de los usuarios o patrocinadores, así como el diseño de soluciones conjuntas, se encuentran porcentajes muy bajos, aun en el sector financiero. Si los usuarios no lideran los proyectos, si estos últimos no tienen un alto grado de evaluación, y si el diseño conjunto de soluciones es bajo, es un reflejo muy fuerte de desconexión.

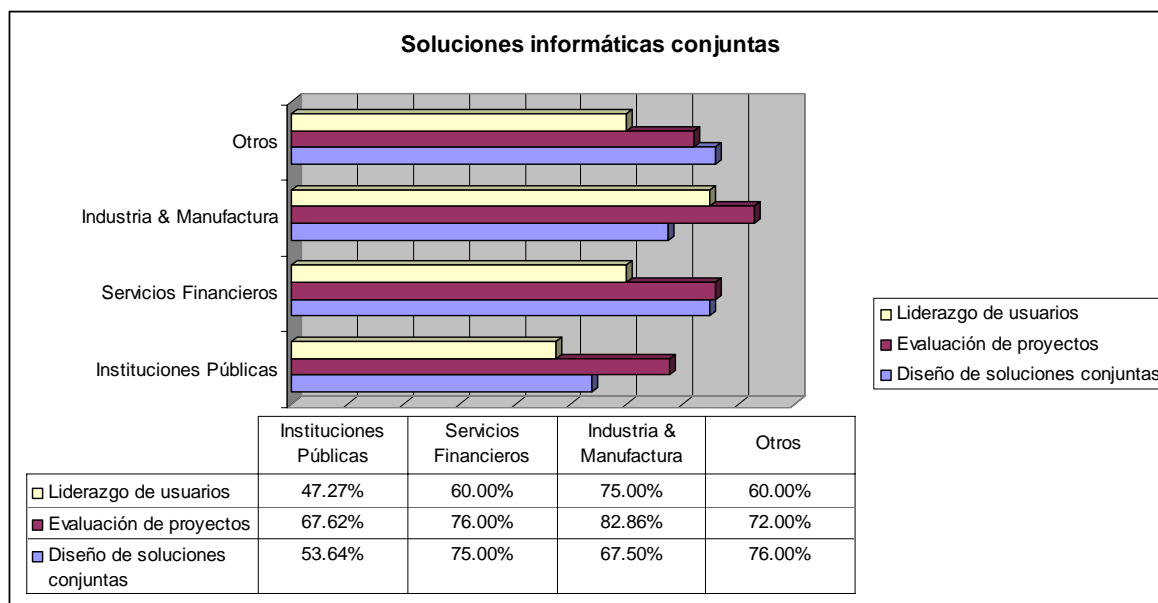
En el sector de industria y manufactura se presenta un porcentaje elevado en lo que a evaluación de proyectos se refiere (82,86%), y esto podría verse como normal porque el negocio fundamental no lo son las tecnologías y, por lo tanto, sus inversiones y gastos tienen que analizarse con mucho detalle para no afectar la rentabilidad del negocio. Por supuesto que lo anterior debería ser válido en el sector financiero, pero la experiencia ha demostrado que a veces el factor FUD (por sus siglas en inglés) ha estado presente en un sector en el que la tecnología es tan importante, en el cual las adquisiciones y compras de productos se hacen con tanta celeridad que a veces no tienen siquiera tiempo de evaluarlas, dado que su ciclo de vida es muy volátil.

El término FUD es un término acuñado a principios de 1960 por los competidores de la empresa más grande del ramo, la IBM. FUD son las primeras letras de las palabras en inglés: miedo, incertidumbre y duda. Había que aterrorizar a los compradores para que adquirieran “mis” productos ya, pues de lo contrario podrían quedar fuera del mercado. O bien, sembrar el terror si trataban de adquirir tecnología que no fuera la de ellos, diciendo que no se harían responsables si se presentaban fallas en los sistemas por adquirir los equipos de la competencia. Para conocer más del tema puede visitarse <http://es.wikipedia.org/wiki/FUD>

Puede verse claramente en el gráfico cómo la participación de los usuarios es relativamente baja. Normalmente esto acarreará consecuencias de aceptación de los sistemas que no se terminen a tiempo, que se extiendan demasiado en sus costos, que haya que redefinirlos constantemente o que no se ajusten a los requerimientos reales del negocio.

El alineamiento que, según se manifestó en el gráfico 2, era muy alto en algunos sectores con esta pregunta de control puede desvirtuarse fácilmente, pues el alineamiento responde a un trabajo conjunto y a una priorización de proyectos; y, por supuesto, a una alta participación de todos los sectores de una organización. En definitiva, existe una desconexión palpable según los gráficos que se han analizado hasta el momento.

Gráfico 7



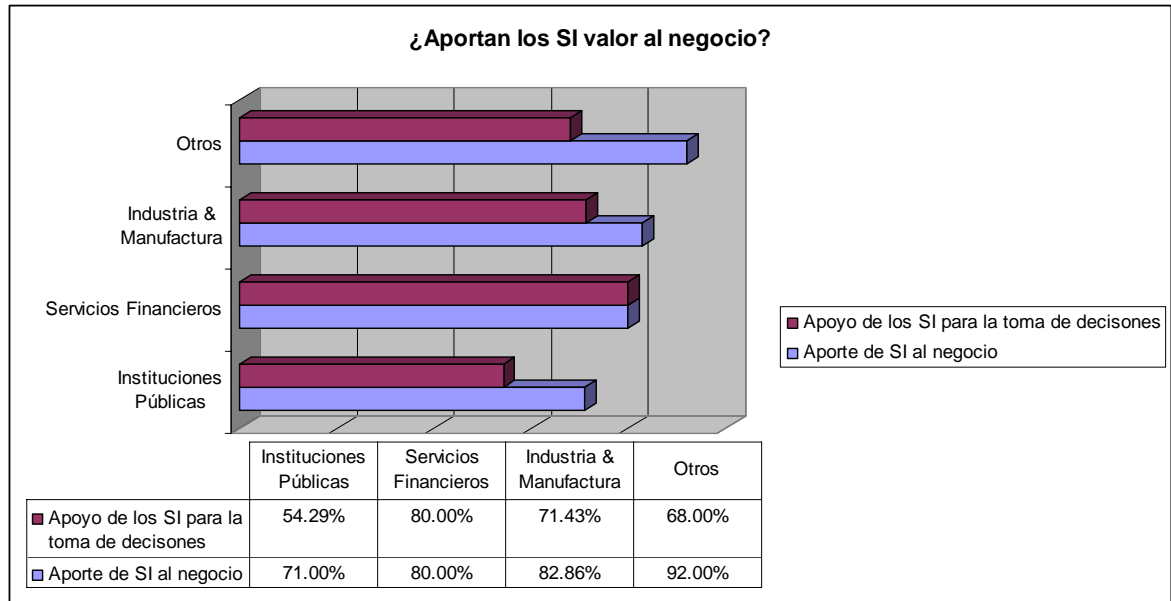
Fuente: Elaboración propia para la investigación

Aporte de valor de los SI al negocio

Uno de los aspectos prioritarios para el desarrollo de sistemas es que éstos aporten valor al negocio y se puede determinar de manera sencilla si facilitan la toma de decisiones. De la investigación se deduce (ver el gráfico 8) que en el sector público (54,29%) y en otros sectores (68%) esto no se aplica, y posiblemente lo que se tiene son sistemas netamente operativos.

Llama la atención que, ante la pregunta de si los sistemas de información aportan valor al negocio, los porcentajes superaron 70%, posiblemente por su aporte en la simplificación de flujos de proceso y registro; pero no por estar dirigidos a facilitar la toma de decisiones. Hay que ser claros en que se dio por sentado que todos entendían lo que es aporte de valor, lo cual puede que no sea cierto. El valor se mide en términos cuantificables, con medidas y métricas, aunque también hay intangibles. Se recomienda visitar http://www.intel.com/it/it-management/#business_value, que trata este tema en forma amplia. También se recomienda la lectura del libro de Martin Curley citado en otro capítulo y que forma parte de la bibliografía.

Gráfico 8



Fuente: Elaboración propia para la investigación

Cultura informática

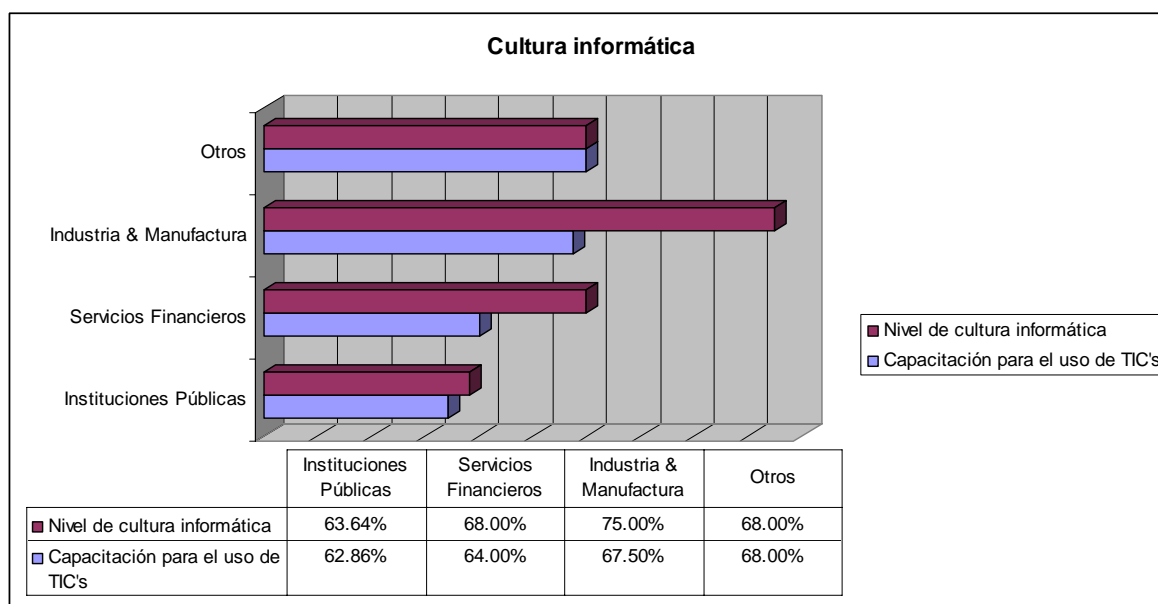
Si existe una apropiada cultura informática en la organización ésta se convierte en un gran aporte al desarrollo de TIC; y si la cultura es fuerte es muy probable que la desconexión sea leve. Si se compara el gráfico 6 -en el ítem sobre conocimiento del PEI- con los indicadores del gráfico 9, se encuentran coincidencias que claramente indican que la divulgación del PEI tiene una relación directa con la capacitación y la cultura informática.

Al ser tan bajos estos indicadores, éstos muestran una desconexión muy importante en los diferentes sectores, y en el caso del sector financiero se da más con respecto a los niveles inferiores. Por supuesto, se acepta que el término cultura informática puede ser ambiguo, si los participantes no conocen en realidad cuáles son los componentes que caracterizan una cultura. Lo que sí queda muy claro y sin lugar a dudas es que la capacitación es muy baja aunque las cifras parecieran altas.

Lo que las personas entienden por capacitación es normalmente es que se les haya enseñado a utilizar paquetes del tipo de procesadores de palabras y hojas de cálculo, o bien, para manejo de presentaciones (*Power point*). Rara vez se les instruye sobre la importancia que tienen en el uso adecuado de las tecnologías sus principales componentes (sistemas de información, sistemas de información ejecutivos, almacenes de datos, inteligencia de negocios, etc.), y cómo las TIC pueden agregar valor al negocio.

La capacitación es un eje fundamental para lograr disminuir los niveles de desconexión, acerca de lo cual posteriormente se dan algunas sugerencias.

Gráfico 9



Fuente: Elaboración propia para la investigación

Comunicación TIC – Administración

El gráfico 10 muestra que, excepto en el sector financiero, el lenguaje informático aplicado en su expresión natural sigue siendo una barrera entre los administradores y los informáticos. Esto lleva a una consecuencia reflejada en el mismo gráfico: no es fácil obtener soluciones con la gerencia de TIC si los porcentajes se mueven entre 55,45% y 72% en el sector financiero.

En el sector público y en el sector de industria y manufactura la barrera del lenguaje es más evidente con porcentajes de 63,81% y 65%, respectivamente. El problema en verdad es serio y es de naturaleza global. Tan es así que en el curso SANS Security Leadership Essentials for Managers with Knowledge Compression, de Sans Institute, 2006, en el tomo VI se dedicó casi la mitad de sus páginas a un glosario de términos que incluso el personal informático no conocía. Es muy

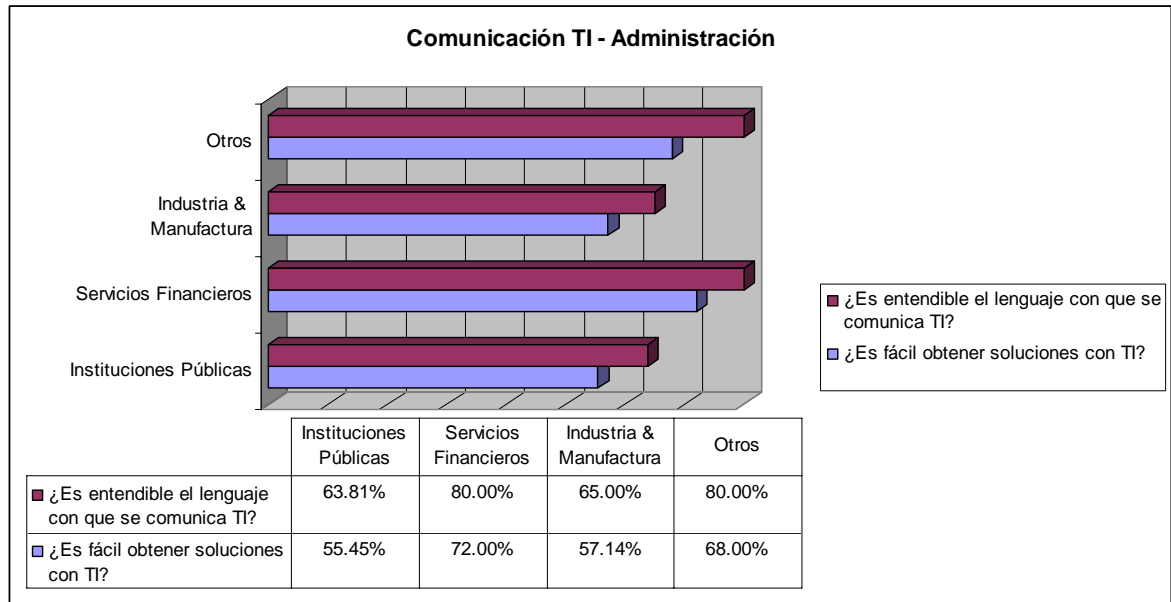
normal encontrar frases como las siguientes: “Este curso está diseñado para que los estudiantes puedan obtener su certificación GSLC o bien la CISSP”; otra más:

“Para garantizar que todos los requerimientos para aplicar el TCO sean aprobados por el CCB, puede utilizar también la metodología BPM”.

Los anteriores términos no son difíciles de entender pero cuando se utilizan algunos como VPN, HLDC, SNMP, ISO/OSI, UDP, PHISSEC, IDS, IPS, etc., que son fácilmente reconocibles por la mayoría de los tecnólogos informáticos, en presencia de administradores; o salen corriendo o no quieren saber nada de lo que se está hablando, y mucho menos reconocer que no entienden absolutamente nada. El lenguaje utilizado genera desconexión. Pero el asunto va en dos direcciones cuando los administradores, especialmente del nivel contable, utilizan su propia jerga.

Una queja común, muy generalizada entre los administradores es que informática no entrega los sistemas adecuados para su negocio, pero lo más grave es que manifiestan que no es sencillo obtener soluciones de parte de TIC, lo cual queda evidenciado en el gráfico 10.

Gráfico 10



Fuente: Elaboración propia para la investigación

Informáticos y “no informáticos”

La tabla 1 muestra los diferentes porcentajes en relación con cada una de las preguntas formuladas en el cuestionario. Se observa claramente que existen algunas brechas entre el pensamiento del personal informático y el del administrativo que reflejan desconexión. Pero queda más claro aun con sus coincidencias en cuanto a que existe una clara desconexión.

Por ejemplo, ante la pregunta de si el liderazgo de los proyectos es ejercido por los usuarios, 49,47% de los informáticos manifestaron que sí, lo cual es muy bajo, mientras que los “no informáticos” respondieron en 61,90%. La desconexión no queda manifiesta por la diferencia de porcentajes sino porque ambas cifras son muy bajas y ambas partes aceptan que no hay un verdadero liderazgo de parte de los usuarios.

Los usuarios deberían tener un mayor liderazgo en este tipo de proyectos, puesto que los sistemas que se desarrollen deben ir en función directa de las “necesidades del negocio”, lo que genera el valor adecuado. Al no mantener un fuerte liderazgo es probable que los informáticos con poca formación en el área

administrativa tomen decisiones de desarrollo que no son las más adecuadas, y entreguen luego “productos” que no van a cumplir con los requerimientos de estos usuarios. Las últimas cuatro preguntas de esta tabla reflejan un alto nivel de desconexión, aceptado por ambos tipos de profesionales.

En términos generales, analizando incluso en forma rápida la información presentada, se puede afirmar que la desconexión es un hecho real. No importa que la alta dirección se sienta orgullosa de sus inversiones en tecnología, lo cual es muy común escuchar, o que incluso muestren a sus contrapartes en otras organizaciones cómo poseen la última de las computadoras personales “lanzadas” al mercado, con gran poder de procesamiento y velocidad y con los últimos adelantos presentados por los fabricantes. Si éstas no agregan valor al negocio y si sólo se utilizan para procesamiento de palabras o para leer sus “correos”, para lo único que están sirviendo, en términos generales, es para mostrar que se tiene el poder económico requerido para adquirirlas; pero ésta no es una razón válida para un negocio en marcha.

Tabla 1

Informáticos y “no informáticos”		
Pregunta	s	No Informáticos
¿Existe un plan estratégico en la empresa?	94,12%	95,24%
¿Se cuenta con un plan estratégico de TI?	64,71%	72,22%
¿Está alineado el PEI con el plan estratégico de la empresa?	83,33%	78,46%
¿Participa TI en el desarrollo del plan estratégico de la empresa?	68,75%	65,88%
¿Comunica TI información importante a sus clientes (planes, cambios)?	67,37%	59,00%
¿Depende el gerente de tecnologías de información (TI) del nivel superior de la organización?	63,16%	40,00%
¿Existe un grupo de alto nivel que priorice el desarrollo de la tecnología?	73,68%	80,95%
¿Se analiza y discute el presupuesto de TI con la gerencia general?	70,00%	68,24%
¿El tema de TI es parte de la agenda del nivel superior de la organización?	74,12%	68,00%
¿Cuál es el nivel de auditoría de sistemas en la organización?	52,22%	56,25%
¿La opinión de TI es considerada en la toma de decisiones que la afectan?	76,84%	72,00%
¿Se elabora el plan estratégico de informática (PEI) de manera conjunta entre los niveles gerenciales de la empresa y TI?	100,00%	76,92%
¿Considera usted que en la organización se conoce el PEI?	58,33%	51,43%
¿Se revisa periódicamente el PEI?	75,00%	61,82%

¿Tecnologías de información y sus usuarios definen soluciones para sus necesidades en conjunto?	64,44%	59,05%
¿Se evalúan los proyectos de tal manera que se desarrollan aquellos que aportan más valor al negocio?	72,63%	71,58%
¿Es ejercido el liderazgo de los proyectos por el usuario?	49,47%	61,90%
¿Aportan valor al negocio los sistemas de información que se desarrollan?	78,89%	75,79%
¿Satisfacen las necesidades de información de los usuarios los sistemas en producción?	75,56%	67,62%
¿Se adaptan fácilmente a las necesidades del negocio los sistemas de información?	70,00%	68,00%
¿Se utilizan los sistemas en producción para apoyar la toma de decisiones?	64,44%	60,00%
¿Conoce los procedimientos para gestionar necesidades o requerimientos ante TI?	68,89%	72,00%
¿Es fácil obtener soluciones con TI?	65,26%	54,00%
¿Analiza TI riesgos y oportunidades que afectan el desarrollo de los negocios?	67,37%	61,11%
¿Cuentan los usuarios con la capacitación suficiente para la utilización de las tecnologías de información de la organización?	65,26%	64,00%
¿Cuenta la organización con políticas institucionales en TI aprobadas?	72,94%	68,42%
¿Existe un nivel elevado de cultura informática en la organización?	64,21%	69,52%
¿Es entendible el lenguaje con que se comunica TI?	71,58%	65,00%

Fuente: Elaboración propia para la investigación

Evaluación sectorial

En la siguiente tabla se presentan los resultados de acuerdo con los niveles sectoriales encuestados. Aquí se denota cómo el sector financiero presenta índices más altos en relación con los otros sectores.

Tabla 2

Evaluación sectorial				
Pregunta	Instituciones Públicas	Servicios Financieros	Industria & Manufactura	Otros
¿Existe un plan estratégico en la empresa?	95,00%	100,00%	100,00%	80,00%
¿Se cuenta con un plan estratégico de TI?	61,11%	100,00%	75,00%	50,00%
¿Está alineado el PEI con el plan estratégico de la empresa?	83,64%	80,00%	74,29%	90,00%
¿Participa TI en el desarrollo del plan estratégico de la empresa?	64,21%	85,00%	63,33%	70,00%
¿Comunica TI información importante a sus clientes (planes, cambios)?	55,24%	64,00%	80,00%	68,00%
¿Depende el gerente de tecnologías de información (TI) del nivel superior de la organización?	50,00%	100,00%	12,50%	75,00%
¿Existe un grupo de alto nivel que priorice el desarrollo de la tecnología?	77,27%	80,00%	100,00%	40,00%

¿Se analiza y discute el presupuesto de TI con la gerencia general?	64,21%	85,00%	60,00%	88,00%
¿Es parte de la agenda del nivel superior de la organización el tema de TI?	67,62%	90,00%	65,71%	76,00%
¿Cuál es el nivel de auditoría de sistemas en la organización?	47,62%	85,00%	56,00%	55,00%
¿Es considerada la opinión de TI en la toma de decisiones que la afectan?	69,09%	92,00%	71,43%	84,00%
¿Se elabora el plan estratégico de informática (PEI) de manera conjunta entre los niveles gerenciales de la empresa y TI?	70,00%	100,00%	100,00%	100,00%
¿Considera usted que en la organización se conoce el PEI?	56,36%	48,00%	51,43%	66,67%
¿Se revisa periódicamente el PEI?	66,00%	80,00%	71,43%	60,00%
¿Definen soluciones a sus necesidades en conjunto tecnologías de información y sus usuarios?	53,64%	75,00%	67,50%	76,00%
¿Se evalúan los proyectos de tal manera que se desarrollan aquellos que aportan más valor al negocio?	67,62%	76,00%	82,86%	72,00%
¿Es ejercido el liderazgo de los proyectos por el usuario?	47,27%	60,00%	75,00%	60,00%
¿Aportan valor al negocio los sistemas de información que se desarrollan?	71,00%	80,00%	82,86%	92,00%
¿Satisfacen las necesidades de información de los usuarios los sistemas en producción?	66,67%	76,00%	80,00%	72,00%
¿Se adaptan fácilmente a las necesidades del negocio los sistemas de información?	62,86%	72,00%	77,14%	80,00%
¿Se utilizan los sistemas en producción para apoyar la toma de decisiones?	54,29%	80,00%	71,43%	68,00%
¿Conoce los procedimientos para gestionar necesidades o requerimientos ante TI?	61,90%	90,00%	72,50%	88,00%
¿Es fácil obtener soluciones con TI?	55,45%	72,00%	57,14%	68,00%
¿Analiza TI riesgos y oportunidades que afectan el desarrollo de los negocios?	57,14%	90,00%	68,57%	68,00%
¿Cuentan los usuarios con la capacitación suficiente para la utilización de las tecnologías de información de la organización?	62,86%	64,00%	67,50%	68,00%
¿Cuenta la organización con políticas institucionales en TI aprobadas?	63,00%	100,00%	77,14%	68,00%
¿Existe un nivel elevado de cultura informática en la organización?	63,64%	68,00%	75,00%	68,00%
¿Es entendible el lenguaje con que se comunica	63,81%	80,00%	65,00%	80,00%

TI?				
-----	--	--	--	--

Fuente: Elaboración propia para la investigación

Con el propósito de tener un marco conceptual amplio que permita entender cómo se van desarrollando en el tiempo las TIC, se hace un resumen de la teoría de las etapas de Nolan, con comentarios relativos a la información obtenida de los gráficos anteriores.

Nolan plantea que existen seis etapas por las cuales pasa la evolución de las TIC, la etapa de inicio, la de contagio, la de control o formalización, la de integración, la de administración de datos y la de madurez.

Hay que resaltar que la mayoría de los informáticos al menos han escuchado de esta teoría; sin embargo, la percepción general es que no le han dado la importancia que en realidad ésta tiene, para entender por qué se presentan ciertos fenómenos relativos a las TIC en las organizaciones.

Se presentan a continuación las características más importantes de las tres primeras etapas. No se incluyen las otras pues si no se ha alcanzado el cumplimiento de éstas difícilmente el de las otras tres, por ejemplo, integración de datos y TIC en forma descentralizada serán alcanzadas.

En la etapa de administración de datos el usuario adquiere la responsabilidad de la integridad de la información y maneja diferentes niveles de acceso. A la luz de la información contenida en los gráficos anteriores, queda en evidencia que la participación de los usuarios no es en ningún caso ni cercana a 90%, por lo que lejos se está de haber alcanzado esta quinta etapa; mucho menos que alguna haya alcanzado su etapa de madurez.

Etapas de inicio

- Comienza con la adquisición de las primeras computadoras y cuya compra se hizo con la finalidad de reducir mano de obra.
- Los primeros sistemas que se empiezan a implantar son transaccionales, tales como planillas, contabilidad y facturación.

- Casi siempre el pequeño departamento de sistemas depende de contabilidad.
- Quien está al frente del departamento es un administrador sin ninguna formación en el área de computación y menos de informática.
- Este departamento cuenta con un analista programador o un analista y un programador que a su vez realizan la operación del equipo de cómputo.
- Se presenta el problema de la ciberfobia, pues el personal teme que sean despedidos al ser desplazados por la computadora.
- La resistencia al cambio se hace presente casi desde los primeros días en que la computadora llega a la organización.

Al realizar la encuesta se notó que algunas organizaciones se encontraban en esta etapa con tendencia a la de contagio, especialmente en el área de industria y manufactura, a pesar de que se consideraba que son organizaciones que cuentan con muchos años de estar en el mercado. La única razón que podría explicar por qué están aún en esa etapa es porque el fenómeno de la desconexión es fuerte en ellas. Al revisar de nuevo algunos indicadores del sector de manufactura se puede tener una idea del estado de algunas de las empresas de dicho sector.

En la siguiente tabla se presentan agrupados los indicadores, en los cuales de un solo vistazo puede notarse que hay bastante desconexión.

Tabla 3

Se cuenta con un PEE y un PEI	75%
Alineación de PEI al PEE	63%
Ubicación de TIC de nivel gerencial	12,50%
Discusión conjunta del presupuesto	60%
Proyector informáticos en la agenda gerencial	65,71%
Nivel de auditoría de sistemas	56%
Conocimiento del PEI en la organización	51,43%
Soluciones informáticas conjuntas	71%

Capacitación para el uso de las TIC	67,50%
¿Es entendible el lenguaje en que se comunica TIC?	65%
¿Es fácil obtener soluciones de TIC?	57,14%

Sólo dos de los indicadores están arriba de 70%. La ubicación de TIC en el nivel gerencial apenas llega a 12,50%, lo que significa que están entre las etapas de inicio y de contagio.

Al esquematizar la segunda etapa lo anterior quedará más claro.

Etapa de contagio

- Se implantan otros sistemas transaccionales, tales como inventarios, control de pedidos y proveeduría, emisión de cheques, etc. Son los primeros intentos de implantar un ERP (*Enterprise Resource Planning*).
- Proliferan las aplicaciones en toda la organización, pero sin control, en forma desordenada.
- Se contrata más personal para el departamento de TIC (que, por supuesto, no lleva este nombre)
- No hay interfases automáticas entre las aplicaciones de un sistema y la salida de otro sistema, se debe realizar el ingreso de la información de salida de un sistema al otro en forma no automática.
- Las aplicaciones se programan con escasez de estándares.
- Los gastos por desarrollo de sistemas crecen de manera importante.

Hay que hacer notar que en una institución bancaria costarricense creada por ley, con aportes de los trabajadores y con más de treinta años de existencia, a pesar de contar con tecnología de muy alto costo y de relativa corta existencia, aún tiene gran cantidad de aplicaciones que interactúan entre ellas de “forma manual”, y no hay interfases entre ellas. Además, muchos de sus “archivos” son

“planos” y no están en bases de datos, con los consiguientes problemas de integridad y de repetición de información. Aunque no era parte de la encuesta, al preguntárseles en qué etapa de Nolan se encontraban respondieron que estaban entre la fase de administración de datos y la de madurez. Se les cuestionó la respuesta y ellos mismos indicaron que tenían problemas de alineamiento, lo cual es cierto, pues la encuesta reflejó niveles de 80% en el caso particular de esa institución.

Etapa de control

- Las aplicaciones están orientadas a facilitar el control de las operaciones del negocio para darles mayor eficiencia.
- El departamento de TIC suele ubicarse en una posición gerencial, y depende normalmente de Finanzas.
- Se establecen prioridades para el desarrollo de nuevas aplicaciones y la cartera de ellas empieza a crecer.
- Se establecen estándares de trabajo, de documentación, de control de proyectos, etc.
- Se inicia el desarrollo de interfases automáticas.
- Nace la planificación de requerimientos de cómputo y de adquisición de recursos computacionales (se han omitido algunas características de esta etapa).

Como se podrá observar, algunas instituciones no cumplen con algunas características de esta etapa, según se desprende del análisis de los gráficos.

El análisis, siguiendo la teoría de las etapas de Nolan, puede ser también un valioso indicador de qué tan desconectada está una organización.

Hay una asociación que no es productiva entre los encargados de TIC y la administración. Esto ha llevado a que haya desilusión o frustración en las organizaciones. Nicholas Carr indica, en un interesante libro, que los ejecutivos

aún no tienen suficiente experiencia ni conocen bien la nueva tecnología, y que tampoco son claras las mejores maneras de evaluar las inversiones y administrar estos activos; y, como resultado, toman decisiones equivocadas en cuanto a la compra y el uso de estas tecnologías. Esto es un reflejo de la desconexión existente.

También se puede afirmar, de acuerdo con la investigación realizada, que, a pesar de las inversiones efectuadas por las organizaciones, nadie se atreve a predecir con un alto nivel de confianza cuál será el resultado de dichas inversiones.

Muchos de los proyectos de TIC se demoran, exceden sus presupuestos o cuando se entregan ya no tienen razón de ser. Es muy probable que esto se deba a la poca interacción que hay entre los encargados de las TIC y la administración.

Cuando se plantea algún proyecto de TIC rara vez se plantea si éste aborda algún problema real del negocio o si le va a agregar algún valor. A veces se adquiere tecnología sin analizar realmente su impacto, por lo que Nicholas Carr también indica que la clave del éxito ya no es buscar una ventaja a toda costa, sino sopesar cuidadosamente los costos y riesgos. Y esto es fundamental, pero es cuando aflora la desconexión.

TIC desea cambiar su tecnología porque considera que es obsoleta y es lo que el mercado indica. Se acepta lo que Nicholas Carr expresa en su libro, en lo que respecta a que los ejecutivos deben considerar los cambios tecnológicos como olas, que los líderes siempre estarán uno o dos pasos adelante de la ola en las aplicaciones o servicios y los seguidores uno o dos pasos atrás. Añade que sería mejor suponer que la inversión en TIC es más baja cada año (no más alta), y luego hacer excepciones cuando la empresa lo requiera. Pero para lograr esto ambas corrientes, tecnólogos y administrativos, deberían “hablarse” o “alinearse” efectivamente.

La desconexión existe aunque esto no se acepte formalmente en las organizaciones. Generalmente se escucha que hay falta de alineamiento en las organizaciones, para hablar en términos positivos; pero eso sólo oculta el problema. En la revista *Computer* de junio del 2006, en un artículo de Lalana

Kagal (del *Massachussets Institute of Technology*), se expresa: “Mientras que los clientes y servicios en los sistemas distribuidos estén físicamente separados y sujetos a que haya desconexión (el subrayado no es del original)...”, lo cual indica que existe este fenómeno como tal. Y más adelante, en el mismo artículo se señala que “...es problemático en estos sistemas debido a la falta de un entendimiento común de requerimientos e información tanto como la “impredecibilidad” de los usuarios”; lo que es otra forma de aceptar la desconexión.

Es muy probable que, aunque no esté explícito en las respuestas a las preguntas del cuestionario, se den muchas de las situaciones que indica Charles B. Wang (:22), como las siguientes:

Quejas de los administradores en relación con los informáticos:

- Se comunican en términos técnicos en vez de hacerlo en términos de negocios.
- Pierden de vista el negocio cuando se trata de decisiones tecnológicas.
- Se mantienen en la ignorancia acerca de los clientes de la compañía y de sus necesidades
 - No mantienen en operación los sistemas claves.
 - Tienen el criterio de que las personas que no son técnicas son dignas de compasión.

Quejas de los informáticos con respecto a los administradores:

- No se sienten cómodos cuando comparten los objetivos estratégicos.
- Se resisten al hecho de tener que reportarse ante la gente de TIC.

- Se niegan a explorar la forma en la cual las TIC los podría ayudar a la resolución de problemas de negocios.
- Insisten en pensar en que las TIC sólo sirven para automatizar funciones contables.
- Se olvidan de tomar en cuenta a los gerentes de TIC para asignarles responsabilidades de negocios.
- Tratan a los profesionales de TIC como si no fueran iguales a ellos.
- Se sienten demasiado inseguros para hacer preguntas técnicas por temor a aparecer como ignorantes.

Todo eso el lector puede constatarlo por sí mismo al recordar cómo se ha sentido cuando ha estado en algún lado de esos mundos. Esas percepciones reflejan no una falta de alineamiento sino una desconexión real entre administradores e informáticos.

En cuanto a la queja de los administradores por la “no comunicación” de los informáticos en términos del negocio, podrían darse varias explicaciones. Los informático rara vez encuentran en sus programas de estudios cursos de administración en los que se tomen en cuenta temas tales como mercadeo, estrategia, administración de los recursos humanos, comportamiento organizacional, etc.; aunque no sea en forma profunda.

Sí se les capacita sobre contabilidad y finanzas; pero esto refleja una desconexión de quienes diseñaron los programas, pues creen que con los cursos técnicos es más que suficiente para que los informáticos entiendan el negocio. Si a esto se suma que los informáticos se quejan de que la administración no los toma en cuenta en aspectos del negocio, la desconexión seguirá creciendo. Además, es difícil lograr que los encargados de las TIC se relacionen con los clientes, pues si en primera instancia no conocen su propio negocio, menos van a conocer el de terceros, y si los mantienen con cierto nivel de aislamiento, entonces la separación no puede eliminarse.

Las quejas de los administradores también son reales. Los términos que se han acuñado por años incluso a veces ya llegan a perder su significado explícito para los tecnólogos. Al aplicar la encuesta se preguntó a un informático que qué significaba, referido a los discos compactos, 20X. Él sabía que era relativo a la velocidad pero ya no sabía el valor de la X. También cuando se le preguntó que qué significaba UDP, pudo decir con certeza que era algo relacionado con un protocolo de comunicación, pero tampoco sabía qué significaban las siglas exactamente. Y eso que eran términos sencillos. Para complicar las cosas se preguntó a alguien que qué significaba DoS (un ataque de denegación de servicios en la red) y ni siquiera tenía una idea de qué se hablaba. Esto es mencionado sólo para ejemplificar que si un administrador quiere entender ese lenguaje no será nada sencillo, pues aunque a veces se sepa qué significan las siglas no es fácil entender el concepto y, para muestra un botón: SSL Secure Socket Layer.

Con la aplicación de la encuesta se logró al menos que algo que está oculto saliera a la luz. Ya queda claro que la desconexión no es un problema técnico sino un problema del negocio. No es un asunto de cambiar a la gente que está al frente de las TIC.

El cuestionario aplicado es sólo un ejemplo. Pueden desarrollarse instrumentos similares, pero lo importante es cerrar las brechas existentes, según lo planteado en cada pregunta, especialmente en aquello que más impacte a una organización en la generación de valor, tanto al cliente interno como al externo. Tampoco es un asunto de buscar culpables, pues ha quedado claro que es un asunto de viajar data.

Charles B. Wang se atreve a asegurar que las organizaciones que eliminan o disminuyen la desconexión “entregan productos y servicios más competitivos. Son más rápidas en llegar al mercado (*time to market*, comentario agregado), tienen costos más bajos y la mayor parte del tiempo toman las decisiones apropiadas. Gastan menos en consultores. Recurren a fuentes externas con menos frecuencia. Reaccionan en una forma más sensible a las condiciones cambiantes.” (:40)

La desconexión -con todas las implicaciones ya analizadas- puede convertirse en una amenaza para la seguridad informática de una organización o en un potenciador de las amenazas, de por sí ya existentes, tal como se describieron en el capítulo 1.

La desconexión como amenaza

De acuerdo con la información presentada en el capítulo cuarto se puede plantear como hipótesis que en cualquier organización es más alta la posibilidad de que la información sufra un ataque en la medida en que la desconexión sea más alta.

En la encuesta no se hizo ninguna pregunta en cuanto a si alguna organización o empresa habría sufrido ataques contra su información. No obstante, lo usual en este campo es que nadie diga que ha sido atacado. Se mencionaba en el capítulo 1 que una de las consecuencias de un ataque puede ser la pérdida de imagen y lo que esto podría acarrear. Por lo tanto, el reconocer que se ha sufrido un incidente es algo que no cualquiera aceptaría. Pese a ello, el autor de este estudio sí cree que hay una relación directa y por eso se propone, a título personal, explicar las razones, lo cual se puede iniciar, incluso, en el mismo orden de los gráficos presentados en el capítulo cuarto.

Durante el segundo semestre del 2006 y el primer trimestre del 2007 se evaluaron 26 planes estratégicos informáticos. Sólo en tres de ellos, correspondientes a instituciones bancarias, había un plan de seguridad. En dos se hablaba algo de seguridad. En los otros no se había tomado en cuenta ningún aspecto de seguridad. Normalmente la seguridad se circunscribió a aspectos tales como adquisición de software para enfrentar el ataque de virus o la limpieza de ellos en equipos comprometidos. Excepto en los que sí contaban con un plan, no habían adquirido paquetes de software para controlar o evitar el ataque de otro tipo de código malicioso, como el de tipo *spyware* o *adware*.

En ninguno había referencias a que existieran políticas expresas para enfrentar el ataque de virus, ni a la utilización del *messenger* en horas laborales con equipos que se utilizan para trabajar, lo cual puede comprometerlos; no había nada con respecto a la protección de la privacidad; la administración de “parches” no seguía ningún procedimiento estandarizado y la utilización del correo para fines personales y el correo personal estaban “por la libre”.

No se encontraron indicios en los planes de que al menos se capacitara al personal en aspectos de ingeniería social, que es uno de los ataques más comunes.

En la mayoría de los planes no existían procedimientos para detectar intrusiones, ni respuesta a emergencias, y menos investigaciones forenses.

Sólo en cuatro de las empresas tenían un oficial de seguridad y sólo dos de ellas contaban con una oficina de seguridad informática.

¿Qué se puede deducir de todo esto?: Que la mayoría de los planes fueron omisos en aspectos fundamentales de aseguramiento de la información por el nivel de desconexión. En una de las instituciones públicas más importantes del país se le preguntó al director de informática por las políticas de seguridad y respondió que eso no estaba en agenda, pues no se consideraba prioritario dado que pensaban que con los equipos que tenían (enrutadores) era suficiente.

En dos textos muy recientes , “los sistemas de información en la empresa actual” (Sandra Sieber y otros) e *Information Systems Strategic Planning* (Cassidy, Anita) se encontró que, pese a ser ambos del año 2006 y a que están orientados al alineamiento estratégico y la planificación estratégica, sólo se hace mención en unos pequeños párrafos a aspectos de seguridad, lo cual puede ser un indicador de que dichos autores, al menos en asuntos de aseguramiento de la información, están “desconectados”. A continuación se citan las referencias de los párrafos (cuantitativamente) en que se menciona algo de seguridad.

Del libro **Planificación**, de Anita Cassidy:

- Nueve líneas en la página 54

- Una línea en la página 247.
- Cuatro líneas en la página 269
- Una línea en la página 270.

El libro de Cassidy, que es, por lo demás, excelente, se usa una gran parte del texto para elaborar un plan estratégico informático. Se mencionan todos los planes necesarios que debe llevar un plan de sistemas de aplicación, un plan de hardware, un plan de software operativo, un plan de equipos de comunicación, etc.; pero brilla por su ausencia el plan de seguridad.

En el de Sandra Sieber y otros:

Diez líneas en la página 151

Una línea como título con seis subítems, página 187.

Igual que en el libro de Cassidy, éste es un material muy importante para entender el alineamiento estratégico de tecnologías con lo objetivos del negocio, y una muy buena guía para elaborar un plan estratégico. Pero también adolece de un defecto sustancial, no dice nada respecto al plan de seguridad.

Por si el lector estuviere interesado en aspectos de planificación de la seguridad con enfoque estratégico, se le sugiere consultar la obra de Vincent Llaveque, ***Information Security***, que se agrega en la bibliografía.

Del gráfico 4 se puede deducir otro aspecto relativo a la seguridad. Si la unidad de TIC no reporta a un nivel superior difícilmente podrá lograr que los aspectos del aseguramiento puedan ser tomados en cuenta.

Para lograr un estándar real, consistente y de buenas prácticas en toda la organización, es necesario que la alta administración dé claras directrices relativas a la seguridad informática y que deje de forma manifiesta su compromiso con tan

importante asunto. Difícilmente, si TIC no tiene esa “cercanía” con un nivel adecuado de la organización, se logrará que en la agenda se incluyan tópicos relativos al aseguramiento de la información; menos logrará que se promueva una política de seguridad de la información que sea aplicada en todos los niveles de la empresa. Si la agenda “corriente” de informática tampoco ocupa un buen lugar en la agenda gerencial, es evidente que los aspectos de seguridad no serán siquiera mencionados.

En el cuadro 5 se presentan los resultados referidos a los comités de informática. En este cuadro se indica que, con excepción del sector de manufactura, hay relativamente pocos comités en funciones en el sector “Otros”, y en los otros dos apenas llega a 80%. Los comités de informática son el preámbulo fundamental para los otros comités, como el de seguridad informática, y normalmente un miembro de este último actúa como enlace en el comité de informática. Si no hay uno de seguridad es muy probable que los aspectos de seguridad que se traten en el de informática sean los corrientes, relativos a la protección antivirus, como ya se ha mencionado; tal vez sobre el uso de métodos de encriptado.

En cuanto al trabajo remoto, es un factor que a veces se deja de lado pero que es muy importante, ya que si se acceden equipos en forma remota y si no se tiene el debido cuidado podrían comprometerse los sistemas. Tampoco se tratarían temas respecto al acceso de terceras partes, comercio electrónico y aspectos relacionados con la tríada C-I-A; no habría diseño de políticas en cuanto a separación de roles y responsabilidades, control de aplicaciones y continuidad de negocios, ni configuración adecuada de estaciones de trabajo, las cuales se dejan con los ajustes por defecto, políticas de respaldo de información, etc.

En el gráfico 9 llama la atención lo relativo a falta de capacitación y al nivel de cultura informática.

En las empresas con cierto tiempo de establecidas, si el papel de la tecnología ha sido limitado o nulo, entonces la cultura es poco receptiva al potencial de las TIC. En estos casos es muy difícil que desde los usuarios operativos hasta los altos mandos estén dispuestos a incorporar en sus labores diarias sistemas más allá de los transaccionales; y sistemas de inteligencia de negocios con todo su gran poder para profundizar en las relaciones que se establecen entre las diferentes entidades de un repositorio de datos o almacén de datos. Aun más, si la empresa ha experimentado fracasos en el desarrollo de sistemas, estará reacia a embarcarse en nuevos proyectos y eso, por lo tanto, se ha erigido en una nueva barrera entre administradores y TIC.

También, si hay poca cultura informática es probable que todo lo que se tenga en cuanto a capacitación sea, más o menos, el manejo de los paquetes estándares de procesadores de palabras o de hojas de cálculo, que se limitan a explotar los aspectos más básicos de dichos paquetes.

Si eso es así, entonces poco se logrará en cuanto a capacitación en aspectos de seguridad; limitado todo a ciertas políticas que impidan la propagación de virus por medios físicos, al utilizar discos compactos (CD-DVD), memorias tipo USB “flash” o los ya casi extintos discos suaves (*floppy disk*).

¿Cómo se puede estar seguro de eso? Con sólo visitar cualquier institución y un poco de ingeniería social se puede determinar que la mayoría de las personas utilizan claves débiles, de menos de ocho caracteres; que en ellas usan nombres propios o que se encuentran en cualquier diccionario, que las escriben en documentos tipo “post it” y las pegan incluso en las pantallas de sus equipos o debajo de su teclado, y que las comparten con sus compañeros o compañeras para que ellos o ellas les ayuden en “algo”. Se podrá observar que abandonan sus puestos de trabajo y dejan las sesiones de sus equipos abiertas. Todo eso son sólo rudimentos, y muy básicos, sobre aspectos de seguridad que no se tratan en las organizaciones.

Lo que se ha comentado hasta el momento facilita que un atacante pueda “hacer fiesta” con tal desprotección, y esto es consecuencia de la misma desconexión, tal como se ha mencionado ya casi hasta la saciedad en esta tesis.

En el gráfico 10 se resumen los problemas de comunicación.

El lenguaje utilizado por los especialistas de seguridad difiere muchísimo del lenguaje propio de los informáticos. Recientemente, en un seminario realizado por la empresa para la cual labora el autor de este estudio, dirigido a los clientes con formación informática, quedó muy claro que prácticamente ninguno de los participantes, que eran más de cincuenta, conocían la jerga de los profesionales en cuanto aseguramiento de la información, la cual se consideran de uso corriente. No pudieron distinguir entre *spyware* y *adware*, entre *phishing* y *pharming*, y tampoco conocían esos conceptos por sí mismos.

Incluso ante términos que se supone que son de uso común, como *hacker* y *cracker*, manifestaron dudas. Sólo para comprobar cuánto conocían se utilizaron los siguientes términos, los cuales eran casi desconocidos por todos: *UDP flood*, *SYN flood*, *ICMP flood*, *smurf attack*, *DoS Attack*, *DDos Attack*, *DNS poisoning*, etc. Si entre profesionales del mismo ramo existe esta desconexión, que no es un pecado, puesto que el aseguramiento de la información es toda una nueva disciplina que se ha convertido en un auge a partir de la segunda mitad de la década de 1990, entonces ¿cómo será con los que no lo son?. Esto no quiere decir que un informático no deba conocer sobre seguridad, pero que este tema no sea abordado en la segunda mitad de la primera década del SXXI sí es un “pecado”.

Existe desconexión y, dependiendo del grado que ésta presente en una empresa, se constituye en una amenaza seria para proteger la información.

La desconexión es tan real como la misma existencia de las TIC en las organizaciones. Pero se pueden seguir estrategias para eliminar su daño en las organizaciones, pues la información que mantienen no es de bajo costo. Además, las organizaciones, como ya se ha comentado, son cada vez más dependientes de esa información.

Si no se acepta la existencia de la desconexión se puede poner en peligro uno de los activos más valiosos -si no el más- de una organización, la información. Y se trata de activos en el sentido verdadero de este término. Se hace esta distinción porque muchos dicen que el activo más importante es la gente. No es adecuado utilizar el término activo para referirse a las personas, pues no son cosas, no son objetos. Es el principal valor de una organización, el capital humano, el capital intelectual, pues lo vale; pero no son un activo.

Algunas estrategias para eliminar la desconexión son tan sencillas que cabe preguntarse: ¿Por qué no se han aplicado? Precisamente por desconocer que hay una “enfermedad”. Si no se tiene conciencia de ella no se aplicará ningún medicamento.

Estrategias para disminuir la desconexión

Teoría de las etapas de Nolan

Una de estas estrategia es analizar en qué etapa de la teoría de Nolan se encuentra la organización y moverse hacia ella. En la medida en que se avanza hacia estadios superiores la desconexión debería ir desapareciendo.

La capacitación como estrategia

Se debería llegar a un tipo de profesional “híbrido”. En el caso de los administradores, que recibieran formación en el campo informático, sin pretender que se conviertan en tales. En el caso de los informáticos, en el campo de la administración.

Este investigador lo ha puesto a prueba durante unos siete años y le ha funcionado perfectamente. En los programas de maestría de la Universidad Fidélitas hay un curso llamado Sistemas de Información Gerencial. Utilizando un texto básico, **Sistemas de información para los negocios**, de Daniel Cohen Karen, con dinámicas en clase para garantizar que se entienden los conceptos, pequeñas investigaciones y un proyecto práctico, se ha logrado eliminar la ciberfobia en todos los estudiantes. Y no se han utilizado más de 40 horas de salón de clase, con la participación de conferencistas invitados, tanto informáticos como administradores, que han tratado temas generales. Al finalizar la experiencia con la aplicación de instrumentos adecuados ha quedado detectado que pueden interactuar de manera apropiada con los informáticos.

En una experiencia relatada por una estudiante, cuyo nombre por razones obvias no se menciona, éste indicó que se había alcanzado el propósito buscado. Ella entrevistó a un director de TIC de un hotel importante de la capital para la realización de su proyecto práctico. La formación de ésta, ahora ex estudiante, era en el área de turismo. El profesional le consultó -después de varias preguntas de ella- en dónde se había graduado en informática; a lo que ella orgullosamente le respondió que era de otra área.

Si eso se puede lograr en un corto seminario, cuánto más se podría alcanzar con la capacitación constante en las organizaciones. La misma experiencia se ha implementado en la carrera de Administración de la Tecnología, en la que se introduce al estudiante en temas propios del campo de la administración, tales como estrategias básicas, planificación estratégica, cadena de valor, pensamiento estratégico, elementos de mercadeo, etc. Los resultados son igualmente sorprendentes.

Cómputo de usuario final (estrategias de CUF)

Con una estrategia de CUF se pueden alinear los objetivos del negocio con la tecnología, porque esto se deja en manos de los que realmente saben o conocen el negocio y sus retos. Los usuarios finales serían los responsables del cuidado, ingreso, procesamiento, etc. de la información, mientras que TIC provee la administración de la tecnología y el manejo óptimo de ella. Con los paquetes de programas con que se cuenta hoy el usuario final puede desarrollar incluso pequeños sistemas, o bien, mediante la adquisición de aplicaciones ya desarrolladas, obtener lo que realmente necesita, mientras que TIC desarrolla lo que el mercado no puede dar.

Proveedores de servicios de aplicaciones

Otro gran recurso que podría utilizarse son los servicios tipo ASP (proveedores de servicios de aplicaciones)

Una de las tendencias modernas va en esa dirección. Se nombra particularmente a la Corporación de Operadores de Servicios Telemáticos (COST, con dirección www.intercoop.fi.cr), la cual patrocinó los estudios del sustentante de esta tesis.

Cost nació como una empresa del tipo ISP (*Internet Service Provider*), con funciones propias de enrutamiento y direccionamiento, almacenamiento de páginas *Web* e instalación de correo electrónico, entre otras cosas. Al asumir la gerencia se inició la transformación de la empresa de un ISP a un ASP. En la actualidad se cuenta con varias aplicaciones que utilizan varios de sus clientes, entre ellas: pago de servicios públicos, envío masivo de mensajes cortos, plataforma electrónica para *Internet Banking*, transferencias de remesas, y pronto entrarán en operación el BPM (*Business Process Manager*) y un software aplicativo para el análisis de riesgos.

Se menciona lo anterior porque esos sistemas los utiliza el personal administrativo sin la participación de informáticos. Ellos se han convertido en los

dueños de las aplicaciones y se ha reducido la dependencia de las TIC propias de las organizaciones clientes. Los sistemas han aportado valor a esas instituciones y empresas, y han contribuido a disminuir la desconexión, pues estas aplicaciones han ayudado a eliminar la ciberfobia y los temas de ellas están en las agendas de los gerentes de alto nivel, ya que los resultados son inmediatos.

Hay varias estrategias para acelerar el cómputo de usuario final y todas ellas deberían ser impulsadas por la administración. Uno de los problemas graves que se encuentran en las organizaciones que contribuyen a la desconexión, además de todo lo que se ha apuntado hasta el momento, es que muchos de los tecnólogos informáticos desarrollan feudos y mantienen en la “ceguera” a los administrativos, lo que alimenta la ciberfobia, pues se han dado cuenta de que al hacerlo aumentan la dependencia de las organizaciones de ellos y, por ende, su poder personal. Aunque esto no es profesional, lamentablemente se da más de lo que se cree.

Descentralización y desconcentración.

Otra estrategia válida para reducir o eliminar la desconexión es mediante la descentralización y desconcentración de la función informática. Lo tradicional ha sido la existencia de enormes centros de informática.

La Universidad de Costa Rica, de carácter estatal y público, inició un proceso de esta naturaleza a principios de los noventa con excelentes resultados. Igualmente, otras universidades públicas imitaron su ejemplo. En el grupo “otros”, en los gráficos presentados se incluyó a las universidades públicas junto con las privadas y con organizaciones que no calzaban dentro de los otros sectores. Por lo tanto, no se puede apreciar el alineamiento logrado en estas universidades públicas. En los datos disgregados se nota que la capacitación, el alineamiento del plan, la participación conjunta y el liderazgo de los usuarios, además de otros indicadores, supera 90% en todos los renglones.

Al dispersarse los recursos se descentralizan las responsabilidades, tan fuertemente marcadas con los grandes centros de informática. Al desconcentrar

los profesionales de las TIC reportan a los gerentes funcionales, lo cual puede lograr una mayor integración de la tecnología con los procesos de los negocios. Se obtienen otros beneficios, se derriba esa pared invisible que existe entre administradores y tecnólogos, ya que el informático aprende rápidamente la jerga de los administradores. Se imbuye más en los problemas de éste y llega a entender mejor su problemática. Del lado de los administradores se logra el mismo efecto, llegan a dominar conceptos y desaparece de manera muy veloz la ciberfobia que pudieran tener. Por supuesto, lo anterior mal manejado puede desembocar en otros problemas. Para evitarlo hay que prestar atención a la cultura existente, y podría darse más bien que los informáticos queden relegados y olvidados, ya que los administradores aumentan las competencias en este campo, y pueden utilizar los servicios tipo ASP o de *outsourcing*.

Cierre de brechas

Una estrategia adicional que se soslayó en otro apartado sería la de tomar cada uno de los indicadores del cuestionario y desarrollar un plan para cerrar las brechas. Para esto se propone el cuestionario utilizado en la encuesta, pero ponderado. Como el valor de cada ítem podría depender de la situación particular de cada institución, se deja para la discusión de los encargados de las TIC, junto con la administración.

Dirección estratégica

“La dirección estratégica –señala Sieber- representa la forma más avanzada y coherente del pensamiento estratégico”. (Sieber, Sandra y otros: 44)

La administración o dirección estratégica extiende el concepto de visión estratégica a lo largo de todas las unidades estratégicas de negocios (UEN) y consolida los valores corporativos, las capacidades y las competencias de los miembros de la organización, las habilidades y las capacidades distintivas; y estas

últimas forman bloques generadores de ventajas competitivas que acoplan en un todo congruente las decisiones de corto, mediano y largo plazos, y eliminan el conflicto C-L al estar impregnado en toda la organización el pensamiento estratégico, que es la base de la planificación estratégica.

Lo anterior logra no solo eliminar el conflicto C-L sino que, al precisar que todos los sistemas que componen la organización estén integrados, permite que la cultura en forma natural pueda alinear los objetivos de todas sus unidades, incluidos los de las TIC, que es lo que se requiere para eliminar la desconexión de los objetivos generales de la organización.

V. CONCLUSIÓN

A lo largo de este estudio debe haber quedado claro que la desconexión es real, que es algo que debe irse eliminado en el transcurso del tiempo, para lograr un retorno adecuado de la inversión que se ha realizado en tecnologías de la información. Si se desea que se agregue valor hay que aplicar algunas de las estrategias enunciadas en el capítulo anterior, o las que se consideren más apropiadas según el tipo de organización; pero debe hacerse. No se puede esperar a que por sí sola desaparezca.

Si las organizaciones no desarrollan procesos de seguimiento de la evolución de las tecnologías, las cuales se desplazan a velocidades que a veces es difícil comprender, excepto por conocer la Ley de Moore, entonces pueden desalinearse de nuevo. Esta ley, formulada por un ingeniero en la década de 1960, que expresa que el poder de computación se duplica cada dieciocho meses, ha probado hasta la fecha ser cierta. Si la tendencia se mantiene y obedece a esta ley, los saltos en el poder de cómputo y lo que se puede hacer con ese poder en términos de desarrollo de aplicaciones es tan amplio que difícilmente sin esa metodología se puede dar seguimiento a la tecnología.

En el tiempo se ha observado que muchos profesionales se quedan con las tecnologías obsoletas porque no han podido actualizarse con la velocidad necesaria, pero la mayoría de las veces ha sido porque las organizaciones no han dedicado recursos a la actualización de ellos.

Lo más grave es que las empresas no tengan personal que esté analizando todas las tecnologías emergentes. Esto no significa que se deben adoptar todas las tecnologías que aparecen constantemente, pero debe analizarse su potencial y aceptarlas o rechazarlas, y no dejar pasar la oportunidad de incorporar nuevas tecnologías por desconocimiento o incapacidad de su personal técnico para incorporarlas efectivamente al negocio.

Se considera que en esta disyuntiva están muchas universidades costarricenses que se mantienen con esquemas tradicionales, aunque podrían incorporar en sus estructuras las facilidades que dan las tecnologías para realizar estudios completamente en línea y en tiempo real, lo que dependería de la carrera; o bien, mixtas con estudios en línea y presenciales. Las que incorporen esta modalidad podrán crecer más que aquellas que sigan con el esquema presencial.

Se percibe que en los próximos veinte años la desconexión puede debilitarse. La brecha digital puede tender a reducirse. Los niños y los jóvenes utilizan Internet en forma intensiva en la actualidad y es de esperar que esto crezca con el paso de los años. Más y más empresas utilizan el *e-Business*, las plataformas electrónicas, para facilitar a los clientes la compra de productos y servicios, lo que permite que las personas pierdan el miedo a la tecnología. Si a esto se suma que cada vez es más sencillo utilizar herramientas informáticas para acceder variado tipo de información y para la toma de decisiones en todo nivel, definitivamente se está de cara a lograr que la desconexión casi desaparezca.

Aunque no hay garantía de que ocurra, si a eso se le agrega una buena dosis de “voluntad” se puede dar por sentado que, en ese plazo o menos, los objetivos de las unidades de TIC estarán completamente alineados con los objetivos de negocios, tal como ocurre con las actividades de apoyo en la cadena de valor, llámense recursos humanos o infraestructura, y las tecnologías son parte de ese tipo de actividades, y no son diferentes.

BIBLIOGRAFÍA

- Carr, Nicholas G. Las tecnologías de la información. Primera edición. Barcelona. Ediciones Urano S.A. 2005.
- Carter, Earl. Cisco Secure Intrusión Detection System. Cuarta Edición. Indianápolis. Cisco Press. 2003.
- Cole, Eric. Insider Threat, protecting the Enterprise from Sabotage, Spying and Theft. Primera Edición. Canada. Andrew Williams. 2006.
- Cassidy, Anita. Information Systems Strategic Planning. Auerbach Publications. Second Edition. USA. 2006.
- Collins, Jim. Good to Great. Harper Business. USA. 2001.
- Dennis, Allan. Networking in the Internet Age. Willey. USA. 2001.
- Edvinsson, L., Malone, M. El Capital Intelectual. Grupo Editorial Norma USA. 1998.
- Forouzan, Behrouz A. Data Communications and Networking. McGraw-Hill. USA. 2003.
- Kaeo, Merite. Diseño de seguridad en redes. Primera edición. Madrid. Pearson Educación S.A. 2003.
- Kay, Trevor. Security+. Primera edición. California. Mc.Graw-Hill. 2003.
- King, C., Dalton, C., Osmanoglu, T.E. Security Architecture. McGraw-Hill. USA. 2001.
- Klevinsky, T.J.;Laliberte, Scott; Gupta, Ajay. Hack I.T. Tercera edición. Boston. Pearson Education, Inc. 2002.
- LeVEQUE, VINCENT. Information Security. IEEE. USA. 2006.
- Nichols, Randall K; Ryan, Daniel J.; Ryan, Julie J.C.H. Defending your digital assets. Primera edición. New York. McGraw-Hill. 2002.
- Northcutt, Stephen; Novak, Judy. Network Intrusion Detection. Segunda Edición. Indiana. New Riders Publishing. 2001.

Pat McCarthy, Mary; Campbell, Stuart y Brownstein, Rob. Seguridad Digital. McGraw-Hill. 2002.

Poulsen, Kevin L. Hack proofing your Network. Segunda Edición. Maryland.Syngress Media, Inc. 2002.

Purba, Sanjiv. New directions in internet management. 2da. Edición. Auerbach. 2002.

Sandra Sieber, Josep Valor, Valentin Porta. Los sistemas de información en la empresa actual. McGraw-Hill. Primera Edición. 2006.

Thompson, Ronald y Cats-Baril, William. Information Tecnology and Management. 2a. ed, McGraw-Hill. 2003

Zagorsky, Jay L., Business Information. Finding and Using Data in the Digital Age. McGraw-Hill. 2003.

ENLACES EN INTERNET

www.rsasecurity.com
www.freebsd.org/security
www.securityfocus.com
www.securityinfowatch.com
www.techsupportalert.com
www.cisco.com
www.infosyssec.com
www.ciac.org
www.cerias.purdue.edu
www.washington.edu/computing/security
www.theiia.org
<http://www.eicar.org/>
<http://www.acm.org/>
<http://www.mitre.org/>
<http://www.hpimg.org>
<http://www.symantec.com>
<http://www.foundstone.com>
<http://www.purge-it.com>
<http://www.stegoarchive.com/>

APENDICE

MEDICIÓN DEL GRADO DE DESCONEXIÓN ENTRE TI Y LA ADMINISTRACIÓN DE LAS EMPRESAS

El propósito de la presente encuesta es medir el grado de desconexión entre los Departamentos de Tecnología de Información y Comunicación y la Administración General de las empresas como parte de un trabajo de investigación para un programa doctoral

Los datos recolectados será manejados con total confidencialidad y las conclusiones se obtendrán no a nivel de empresas o instituciones sino a nivel de sectores.

Muchas gracias por su colaboración.

Cuestionario aplicado

Universidad Fidélitas Maestría en Gestión de la Tecnología

MEDICIÓN DEL GRADO DE DESCONEXIÓN ENTRE TI Y LA ADMINISTRACIÓN DE LAS EMPRESAS

El propósito de la presente encuesta es medir el grado de desconexión entre los Departamentos de Tecnología de Información y la Administración General de las empresas como parte de un trabajo de investigación en el curso Planeamiento Estratégico.

Los datos recolectados será manejados con total confidencialidad y las conclusiones se obtendrán no a nivel de empresas o instituciones sino a nivel de sectores.

Muchas gracias por la colaboración.

¿Labora usted en el departamento de Tecnologías de Información se su empresa?	SI []	NO []
---	--------	--------

¿Cuál es el sector al que pertenece la empresa donde usted labora?	
▪ Institución Pública	[]
▪ Servicios Financieros	[]
▪ Energía y Telecomunicaciones	[]
▪ Industria y Manufactura	[]
▪ Otro, por favor indique cuál: _____	[]

Pregunta Marque SI o NO según corresponda			NR
1	¿Existe un plan estratégico en la empresa?	NO [] SI []	[]
2	¿Depende el gerente de Tecnologías de Información (TI) del nivel superior de la organización?	NO [] SI []	[]
3	¿Existe un grupo de alto nivel que priorice el desarrollo de la tecnología?	NO [] SI []	[]
4	¿Se cuenta con un Plan Estratégico de TI? Si la respuesta es NO por favor pase a la pregunta #9	NO [] SI []	[]
5	¿Se elabora el Plan Estratégico de Informática (PEI) de manera conjunta entre los niveles gerenciales de la empresa y TI?	NO [] SI []	[]

Pregunta Marque con una X una de las casillas que están a la derecha de cada pregunta, "1" representa la calificación más baja y "5" la calificación más alta		1	2	3	4	5	NR
6	¿Está alineado el PEI con el Plan Estratégico de la empresa?	[]	[]	[]	[]	[]	[]
7	¿Considera usted que en la organización se conoce el PEI?	[]	[]	[]	[]	[]	[]
8	¿Se revisa periódicamente el PEI?	[]	[]	[]	[]	[]	[]
9	¿Participa TI en el desarrollo del Plan Estratégico de la empresa?	[]	[]	[]	[]	[]	[]
10	¿Tecnologías de información y sus usuarios definen soluciones a sus necesidades en conjunto?	[]	[]	[]	[]	[]	[]
11	¿Se analiza y discute el presupuesto de TI con la gerencial general?	[]	[]	[]	[]	[]	[]
12	¿El tema de TI es parte de la agenda del nivel superior de la organización?	[]	[]	[]	[]	[]	[]
13	¿Se evalúan los proyectos de tal manera que se desarrollan aquellos que aportan más valor al negocio?	[]	[]	[]	[]	[]	[]
14	¿El liderazgo de los proyectos es ejercido por el usuario?	[]	[]	[]	[]	[]	[]
15	¿Los sistemas de información que se desarrollan aportan valor al negocio?	[]	[]	[]	[]	[]	[]
16	¿Los sistemas en producción satisfacen las necesidades de información de los usuarios?	[]	[]	[]	[]	[]	[]

17	¿Los sistemas de información se adaptan fácilmente a las necesidades del negocio?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
18	¿Se utilizan los sistemas en producción para apoyar la toma de decisiones?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
19	¿Cuentan los usuarios con la capacitación suficiente para la utilización de las tecnologías de información de la organización?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
20	¿Cuenta la organización con políticas institucionales en TI aprobadas?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
21	¿Cuál es el nivel de auditoría de sistemas en la organización?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
22	¿Existe un nivel elevado de cultura informática en la organización?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
23	¿Conoce los procedimientos para gestionar necesidades o requerimientos ante TI?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
24	¿Es entendible el lenguaje con que se comunica TI?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
25	¿La opinión de TI es considerada en la toma de decisiones que le afectan?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
26	¿Es fácil obtener soluciones con TI?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
27	¿Comunica TI información importante a sus clientes (planes, cambios)?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
28	¿TI analiza riesgos y oportunidades que afectan el desarrollo de los negocios?	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

GLOSARIO

ASP (*Application Service Provider*, “proveedor de servicio de aplicaciones”) compañía que hospeda en las instalaciones de sus propios servidores, aplicaciones de software para otras compañías

Bomba lógica programa malicioso que se activa en un tiempo determinado o mediante un disparador

Contraseña Palabra o código utilizado como medida de seguridad contra el acceso no autorizado de los datos.

DDoS (*Distributed Denial of Service* “denegación distribuida de servicios”) Un tipo de ataque de denegación de servicio que acapara miles de sistemas informáticos, con el propósito de lanzar un ataque de forma simultánea y masiva a un sitio **web**

DNS (*Domain Name Server* “servidor de nombres de dominio”) Servicio de Internet que traduce los nombres de dominio a direcciones **IP**.

DoS (*Denial of Service*, “denegación de servicios”) Estado en el que un sistema no puede responder pues ha sido “atacado” con gran cantidad de solicitudes de servicios, haciendo lento el servicio al haberse saturado.

Firewall (Cortafuegos) sistema diseñado para impedir el acceso no autorizado hacia o desde una red privada, en concordancia con las políticas de la organización

Hacker (pirata informático) Individuo que en forma maliciosa ingresa en los sistemas de cómputo sin autorización.

Ingeniería social Capacidad de un individuo de obtener información a través de la persuasión, la manipulación o el engaño, con el propósito de obtener contraseñas o privilegios de acceso a los sistemas de información.

IP (*Internet protocol* “protocolo de Internet”) Protocolo de comunicación de datos de muy amplio uso en el mundo actual, es el protocolo básico de Internet y de muchas otras redes.

ISP (*Internet Service Provider* “proveedor de servicios sobre Internet”) Compañía que proporciona servicios sobre Internet.

Paquete Combinación de una “cabecera” con información de identificación y un “cuerpo”, que contiene los datos que se van a transmitir

Router (enrutador) Un dispositivo que direcciona el tráfico de una red entre redes locales o redes de área extendida, basada en la información provista en los encabezados de los paquetes que se envían.

SNMP (*Simple Network Management Protocol* “Protocolo Simple de Transferencia de correo”) Conjunto de protocolos para administrar redes complejas, funciona enviando mensajes a diferentes partes de una red.

SSL (*Secure Sockets Layer* “Capa de Conectores Seguros) Un protocolo utilizado para encriptar y autenticar sesiones a través de la web.

Troyano (*TrojanHorse* “Caballo de Troya”) Un programa que en apariencia no produce daño, o que aparenta ser beneficioso, pero que en el fondo tiene “intenciones siniestras”.

UDP (User Datagram Protocol) Un protocolo de capa de transporte que envía en forma no confiable paquetes a través de la red, es utilizado por el DNS para efectuar consultas o dar respuestas, también para transmitir aplicaciones de vídeo o de audio.

Virus Un programa que puede “infestar” otros programas introduciendo código malicioso, evolucionando y produciendo copias de sí mismo.

Worm (gusano). Un programa que se replica de manera independiente, pasando de computador en computador a través de la red, produciendo daños en los computadores mientras se propaga.