MILTON F. MARIN CEDEÑO
UD3248SCC7949

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

A Final Thesis Presented to
The Academic Department
of The School of Science and Engineering
in Partial Fulfilment 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 las encuestas, sus análisis y observaciones, preparación de gráficos, sus aportes y comentarios, trabajo de campo efectuado como parte de su proyecto de clase en el programa de Maestría de la Universidad Fidélitas.

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 bendiga.

ÍNDICE

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

RESUMEN EJECUTIVO

La desconexión es el tema que se aborda en esta Tesis y en él se relacionan varias dimensiones que por lo general no se abordan cuando se habla de ella y es prácticamente desconocido, por una gran mayoría del personal de las organizaciones. Un concepto similar es el de no alineamiento entre las Tecnologías de Información y Comunicación (TIC) y los objetivos estratégicos de una organización.

El concepto de la desconexión es más que no alineamiento, es, además de esto último, un problema serio de comunicación entre los profesionales tecnólogos de las TIC y los no tecnólogos o personal administrativo; un problema de una cultura dentro de una cultura mayor que aunque a veces intentan "caminar" juntas, en ocasiones toman caminos diferentes en detrimento de los intereses últimos de una organización; también, es un "doble discurso", la Alta Dirección justificando las inversiones en TIC pero sin comprometerse en la administración estratégica de ellas.

Esta tesis midió el grado de desconexión existente entre los profesionales de la tecnología informática y el resto de la organización, y dejará en claro que este problema potencia las amenazas que se ciernen sobre la información, que en la medida en que la desconexión cree una brecha de mayores proporciones, en esa misma medida la información puede estar "comprometida", que se maximizarán las amenazas que están presentes tanto en el ambiente externo como en el interno y las vulnerabilidades que existen en las aplicaciones y en el manejo o cuidado de dicha información.

Se realizaron varias encuestas para demostrar que la problemática descrita brevemente en los párrafos anteriores en realidad sí se da efectivamente en las organizaciones de cualquier naturaleza. En la primera se utilizaron indicadores

para medir el grado de desconexión presente en las organizaciones. 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 prepararon varios gráficos para presentar en forma visual los hallazgos. Posteriormente se realizaron otras encuestas que ampliaron las primeras observaciones, más específicamente en aspectos de cultura informática y de la importancia relativa de los comités de informática en una organización.

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, potencia las amenazas tanto de orden externo como externo y que las organizaciones deben enfrentarla con diferentes estrategias para cerrar esa brecha, la cual podría de alguna manera disminuirse en forma “natural”, pero que no será suficiente si no se realizan esfuerzos en ese sentido, para cerrarla completamente.

Se reconoce que el trabajo de preparación de los indicadores, de las encuestas, trabajo de campo, diseño de gráficos, fue elaborado por estudiantes de maestría de la Universidad Fidélitas, bajo la supervisión del proponente, como parte de sus proyectos de clase; ninguno de esos trabajos eran parte de sus proyectos de graduación, sino asignaciones propias del curso.

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 Internet y su exponencial crecimiento y utilización, especialmente desde los inicios de la década de los noventa, las preocupaciones básicas aumentaron en forma considerable, pues aparecieron 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 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 último 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.; 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).

Se puede afirmar con propiedad que el aseguramiento 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, una estrategia que se ha planteado en el Plan Estratégico de Tecnologías de Información (PETI o PEI) de una organización que ha sido estructurado partiendo de los lineamientos de un Plan Estratégico Empresarial o Institucional (PEE) (alineamiento estratégico).

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, 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 la red puede "mirar" cualquier otro sistema que esté en ella. En el principio esto no era un asunto tan importante, porque la información sensitiva no era fácilmente accesible, pero conforme Internet crecía las compañías cada vez más frecuentemente accesaban 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 IDS, IPS), 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 qué 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).

El 7 de agosto de 2007, Computerworld informó que Verisign Inc. una firma de seguridad muy posicionada en el mercado mundial, confirmó que a uno de sus ya ex colaboradores (se dice que renunció) le habían robado una computadora portátil (l*aptop*) en el mes de julio 2007. Dicha computadora, según Lisa Malloy, funcionaria de dicha empresa, podría contener información personal de sus colaboradores actuales, números de seguro social, fechas de nacimiento, información salarial, números de teléfono y las direcciones de sus hogares.

En fin, información suficiente que podría causar daño a más de uno de los colaboradores actuales de Verisign Inc. Sin obviar lo anterior, el daño a la imagen de una entidad que se supone es especialista en seguridad de la información, ¿en cuánto se puede estimar? ¿Cuánto se puede confiar en ella a partir de un hecho como este?

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 este aparte en cuanto al valor de la información, hay que resaltar que dicho valor 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.

Según McCarthy, "la seguridad informática se basa en tres componentes las personas, los procesos y tecnología" (:32), y esto es un asunto de 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 ella, han sido no sólo la poca participación de la Alta Dirección (AD) en aspectos relacionados con la tecnología sino también al desconocimiento que ésta tiene de los términos y de los problemas propios de la informática.

Lo anterior ha desembocado en que la AD 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).

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 externas 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; no conectándose a Internet o no trabajando en red; pero tales medidas estarían fuera de la realidad.

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."[1]

Disponibilidad:

[1] (Traducción libre) (Kay:203

"Que la información esté libre para ser utilizada por los usuarios autorizados cuando fuere requerida".[2]

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 los 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

[2] (Nichols:45)

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."[3]

> 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".[4]

[3] (Kay:204)
[4] (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).

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."[5]

El anterior concepto según lo define el señor Wang es falta de alineamiento o no alineamiento. Se sabe que en realidad hay un fenómeno que separa a estos dos tipos de ejecutivos, tecnólogos y no tecnólogos y aunque no han utilizado este concepto en forma explícita o quizás lo han llamado con otro nombre, nadie duda de su existencia. Se insiste, desconexión es más que no alineamiento.

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 se expone en esta Tesis. 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.

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 y a una subcultura (la de tecnología) que es a veces un mundo aparte al de la organización y que cree ser independiente de ella; por otro lado, una cultura "general" que no logra entender que la tecnología es un elemento de la cadena de valor y una actividad de apoyo, tal como lo es la infraestructura o el departamento de recursos humanos.

[5] (Wang:1)

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."[6]

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. para su personal del área informática diferentes a la del resto de la organización. 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

[6] (Wang:26)

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 de esa manera o como se esperaba.

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 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 utilizaciones crecientes de TI/SI, pero sin un proceso claro de planificación de ella. 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**…"[7]

Más adelante indican ellos mismos:

[7] (Fin de la cita, el resaltado no es del original)(Valor:4).

> "Para aquellas empresas que han logrado derribar la pared que tradicionalmente aísla al departamento de SI del resto se abren nuevas oportunidades"[8]

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

Las amenazas a la información

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

La pregunta que debe obligatoriamente debe 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.

[8] (Valor:5).

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 impulsadores 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 electric	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

Tabla 1
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 threat* 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.[9]

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 el Dr. Eric Cole,

“el verdadero culpable es el atacante, no la víctima”[10]

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.

[9] Tomado de Internet: ***blnews.com/txt/noticia.php?id=131812 S***
[10] (Cole:5).

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"[11]

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".

[11] (Traducción libre del autor de este estudio).

Tampoco hay que dejar de lado que un *insider* o colaborador puede comprometer la información por descuido o por no cumplir con las normas, políticas o procedimientos, tal como sucedió con el caso de Verisign.

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 **II Marco Conceptual y Definición de la Investigación**, en el que se define el concepto de esta investigación.

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.

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 **II** 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 fue mediante un acercamiento a distintos colaboradores en las organizaciones que se escogieron de acuerdo a una muestra seleccionada a conveniencia que se constituyó en el universo para verificar el efecto "desconexión". Fue aplicado de manera profesional a aquellas personas de un total de cuarenta instituciones que estuvieron 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.

Posteriormente se preparó tomando como base los indicadores anteriores, otro conjunto de indicadores que permitieran ponderar el grado de desconexión de una organización. Se aplicó una encuesta en este sentido sólo a cuatro empresas para su validación y se obtuvieron resultados que se explican más adelante.

De la misma manera, se realizaron otros estudios complementarios para profundizar aún más en el tema de la desconexión según se plantea en esta tesis.

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.

Limitaciones de las encuestas

Ventajas de las encuestas

Conformación de temas

Encuesta: Medición del grado de desconexión entre TI y la administración de las empresas

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

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

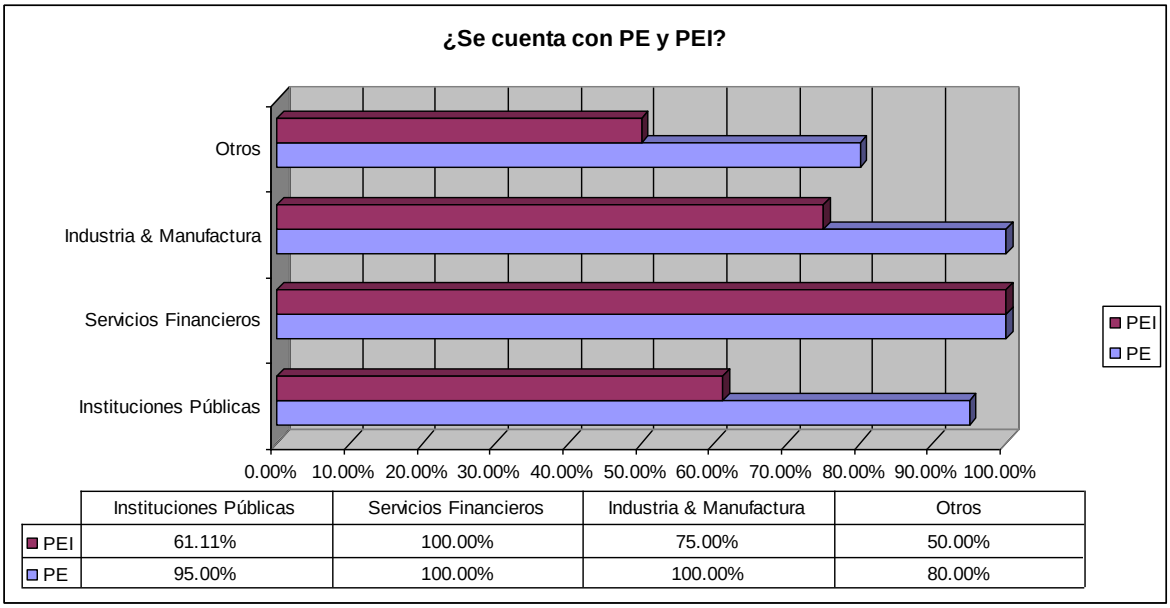
El alineamiento del plan estratégico informático (PEI) con el plan estratégico de la empresa (PEE) puede lograrse de dos maneras, en forma pasiva o en forma activa. La forma pasiva consiste en definir el PEI a partir de la estrategia corporativa y las necesidades concretas de cada unidad de negocio.

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



	Instituciones Públicas	Servicios Financieros	Industria & Manufactura	Otros
PEI	61.11%	100.00%	75.00%	50.00%
PE	95.00%	100.00%	100.00%	80.00%

Ilustración 1
Fuente: Ver reconocimientos

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.

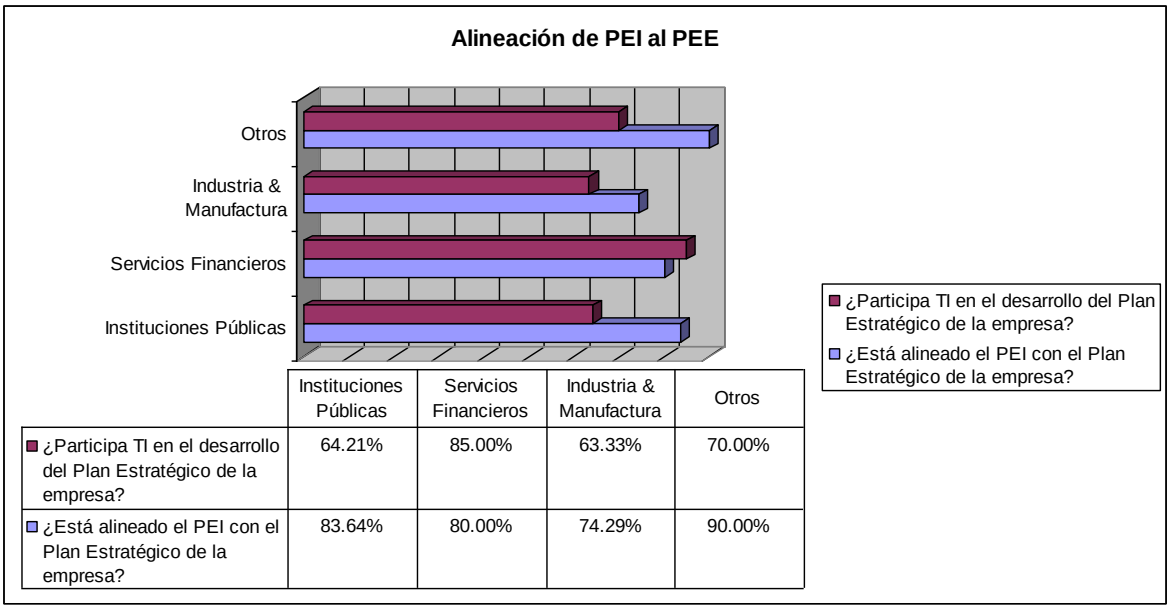
En el sector financiero, que cuenta con 100% de PEI y PEE, existe una falta de alineamiento de 20%. Independientemente del nivel de desconexión, es un problema que debiera ser analizado cuidadosamente por esas instancias, dado que en este sector la intensidad de la rivalidad es muy alta, las fusiones 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



	Instituciones Públicas	Servicios Financieros	Industria & Manufactura	Otros
¿Participa TI en el desarrollo del Plan Estratégico de la empresa?	64.21%	85.00%	63.33%	70.00%
¿Está alineado el PEI con el Plan Estratégico de la empresa?	83.64%	80.00%	74.29%	90.00%

Ilustración 2
Fuente: Ver reconocimientos

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.

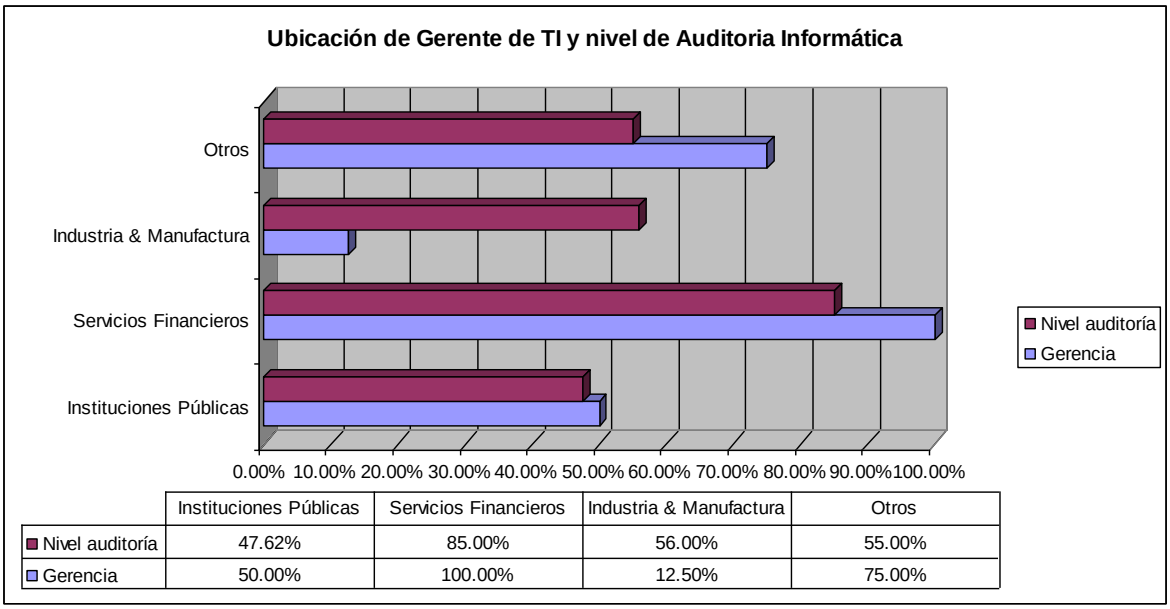
En las instituciones de corte financiero 100% de los directores de TIC reportan a la alta dirección; pero, como se verá adelante, tampoco es indicativo de que la alta dirección esté "alineada" con la tecnología. De hecho, 10% de instituciones que no tienen un lugar en la agenda para asuntos de tecnología. 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



	Instituciones Públicas	Servicios Financieros	Industria & Manufactura	Otros
Nivel auditoría	47.62%	85.00%	56.00%	55.00%
Gerencia	50.00%	100.00%	12.50%	75.00%

Ilustración 3
Fuente: Ver reconocimientos

Análisis y revisión presupuestaria

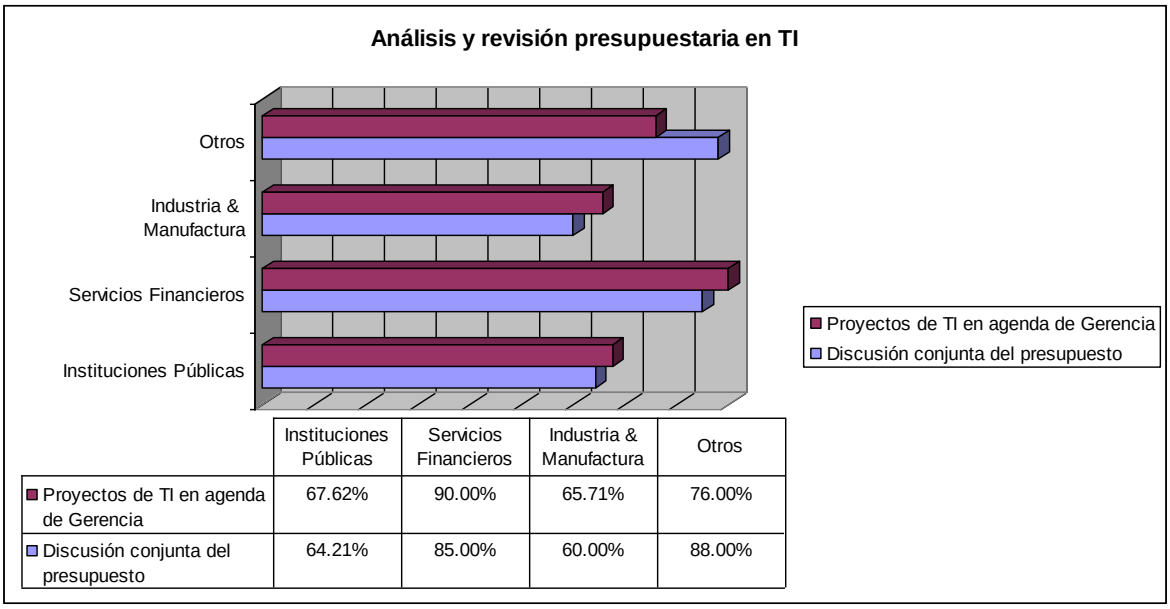
Es normal escuchar a gerentes de TIC decir que sus presupuestos fueron recortados sin consultarles o que no fueron aprobadas todas sus peticiones. Generalmente esto sucede por la falta de presencia de TIC en la agenda de la organización.

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



	Instituciones Públicas	Servicios Financieros	Industria & Manufactura	Otros
Proyectos de TI en agenda de Gerencia	67.62%	90.00%	65.71%	76.00%
Discusión conjunta del presupuesto	64.21%	85.00%	60.00%	88.00%

Ilustración 4
Fuente: Ver reconocimientos

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.

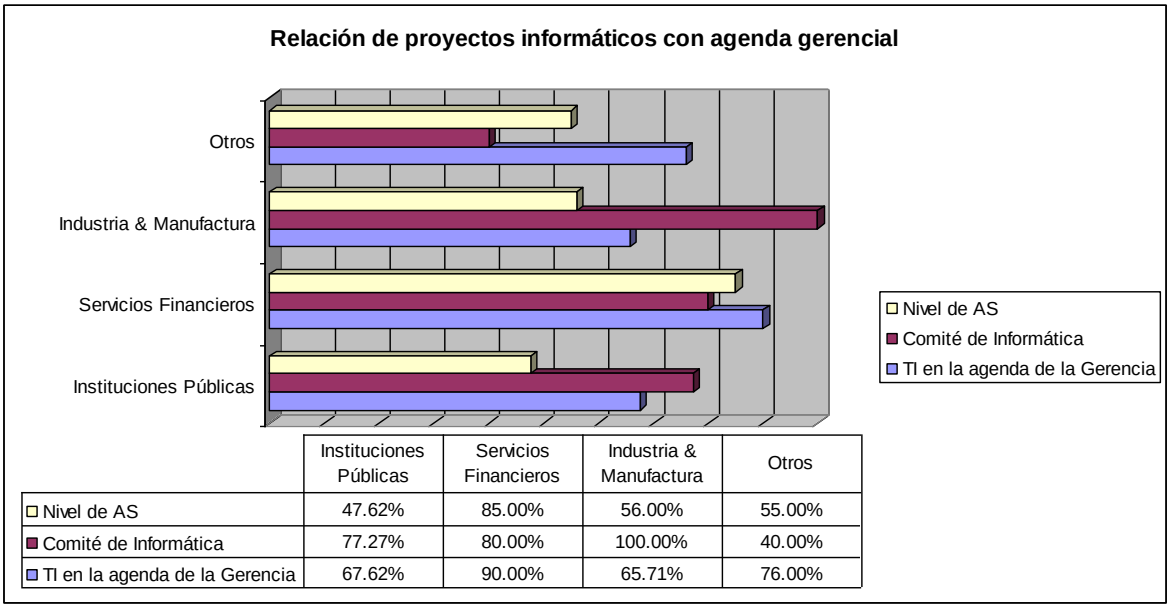
Si se efectúa un análisis más detallado pueden observarse “disonancias”. Por ejemplo, en el sector manufactura se cuenta con un comité de informática en 100% de los casos. Sin embargo, los temas relacionados con informática sólo están presentes en menos de 66%. Habría que preguntarse por qué se da esta 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



	Instituciones Públicas	Servicios Financieros	Industria & Manufactura	Otros
Nivel de AS	47.62%	85.00%	56.00%	55.00%
Comité de Informática	77.27%	80.00%	100.00%	40.00%
TI en la agenda de la Gerencia	67.62%	90.00%	65.71%	76.00%

Ilustración 5
Fuente: Ver reconocimientos.

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.

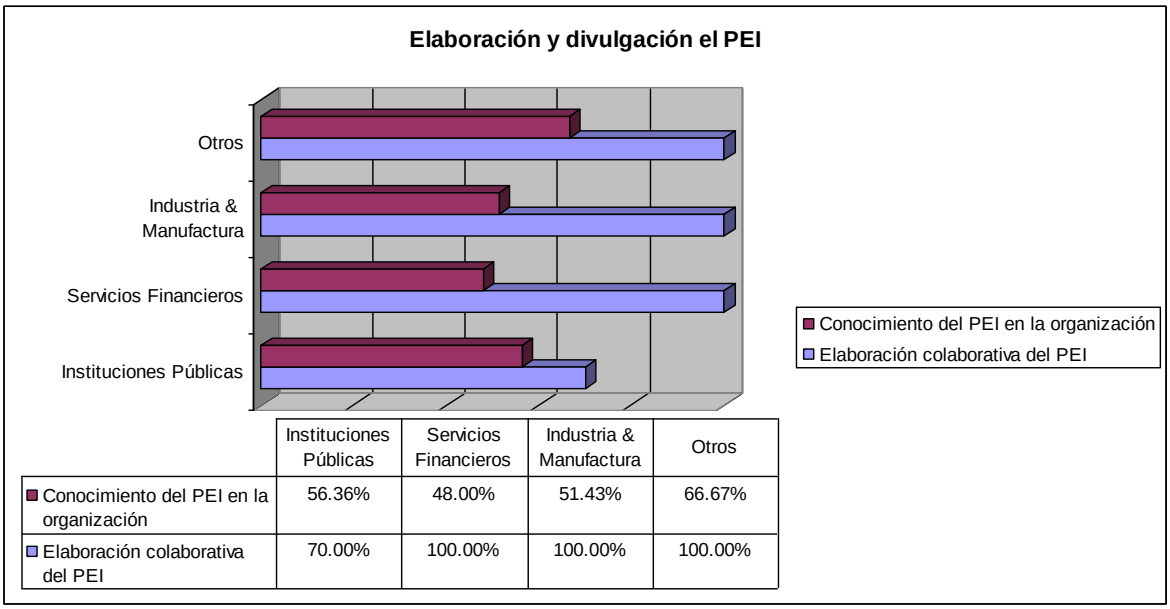
Por otro lado, si no hay participación de todas las partes involucradas en las TIC, igual se pueden tener diferentes grados de desconexión y lógicamente un plan incompleto. Sin embargo, la investigación arrojó un dato interesante: la participación es altísima en todos los sectores y la divulgación muy 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



	Instituciones Públicas	Servicios Financieros	Industria & Manufactura	Otros
Conocimiento del PEI en la organización	56.36%	48.00%	51.43%	66.67%
Elaboración colaborativa del PEI	70.00%	100.00%	100.00%	100.00%

Ilustración 6
Fuente: Ver reconocimientos

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 jerarcas 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.

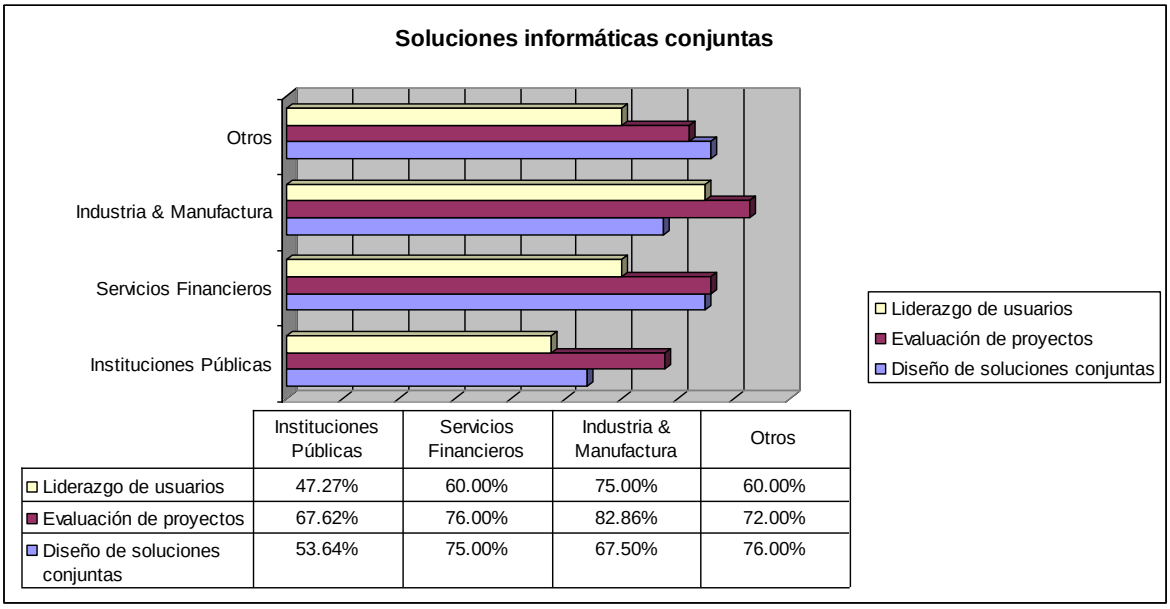
El término FUD es un término acuñado a principios de 1960 por los competidores de la empresa más grande del ramo, la IBM. FUD son las primeras letras de las palabras en inglés: miedo, incertidumbre y duda. Había que aterrorizar a los compradores para que adquirieran “mis” productos ya, pues de lo contrario 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



	Instituciones Públicas	Servicios Financieros	Industria & Manufactura	Otros
Liderazgo de usuarios	47.27%	60.00%	75.00%	60.00%
Evaluación de proyectos	67.62%	76.00%	82.86%	72.00%
Diseño de soluciones conjuntas	53.64%	75.00%	67.50%	76.00%

Ilustración 7
Fuente: Ver reconocimientos

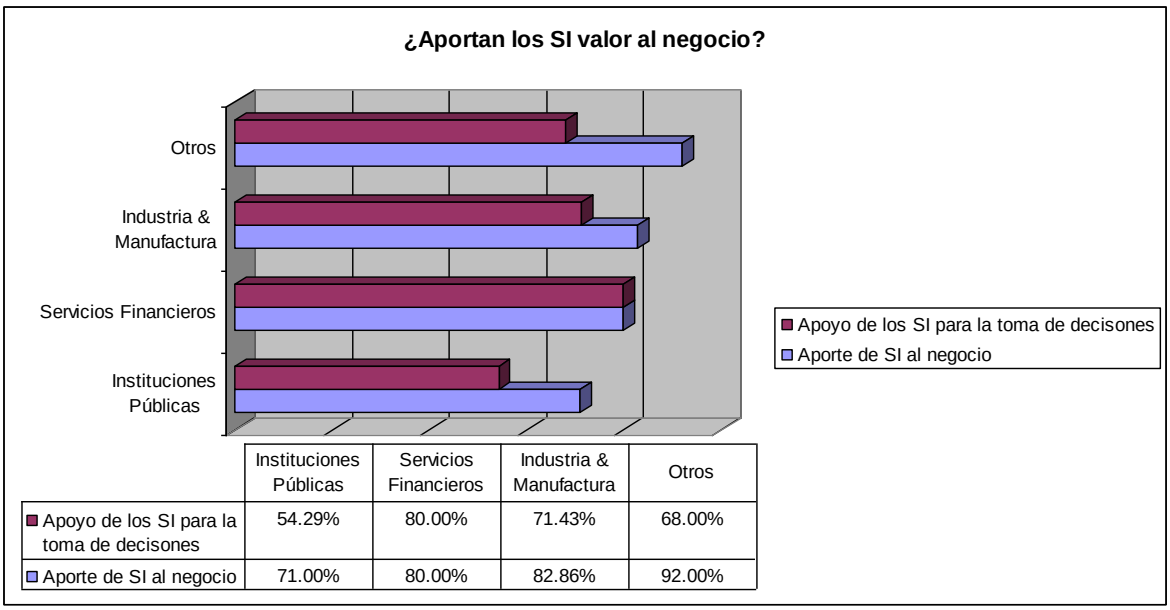
Aporte de valor de los SI al negocio

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



	Instituciones Públicas	Servicios Financieros	Industria & Manufactura	Otros
Apoyo de los SI para la toma de decisones	54.29%	80.00%	71.43%	68.00%
Aporte de SI al negocio	71.00%	80.00%	82.86%	92.00%

Ilustración 8
Fuente: Ver reconocimientos

Cultura informática

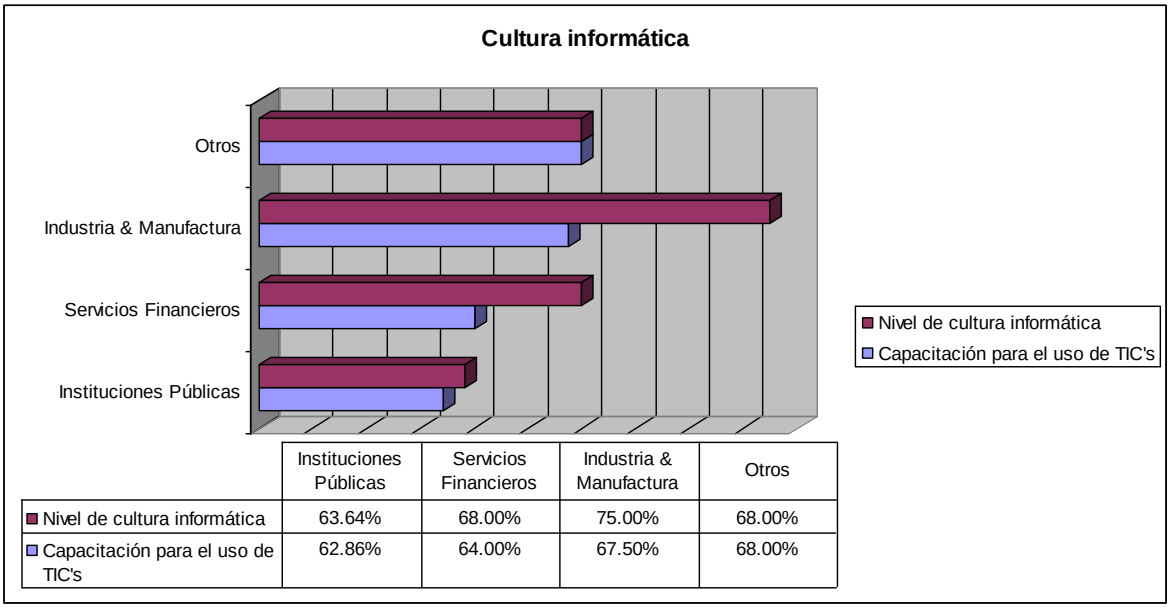
Si existe una apropiada cultura informática en la organización ésta se convierte en un gran aporte al desarrollo de TIC; y si la cultura es fuerte es muy probable que la desconexión sea leve. Si se compara el gráfico 6 -en el ítem sobre conocimiento del PEI- con los indicadores del gráfico 9, se encuentran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



	Instituciones Públicas	Servicios Financieros	Industria & Manufactura	Otros
Nivel de cultura informática	63.64%	68.00%	75.00%	68.00%
Capacitación para el uso de TIC's	62.86%	64.00%	67.50%	68.00%

Ilustración 9
Fuente: Ver reconocimientos

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.

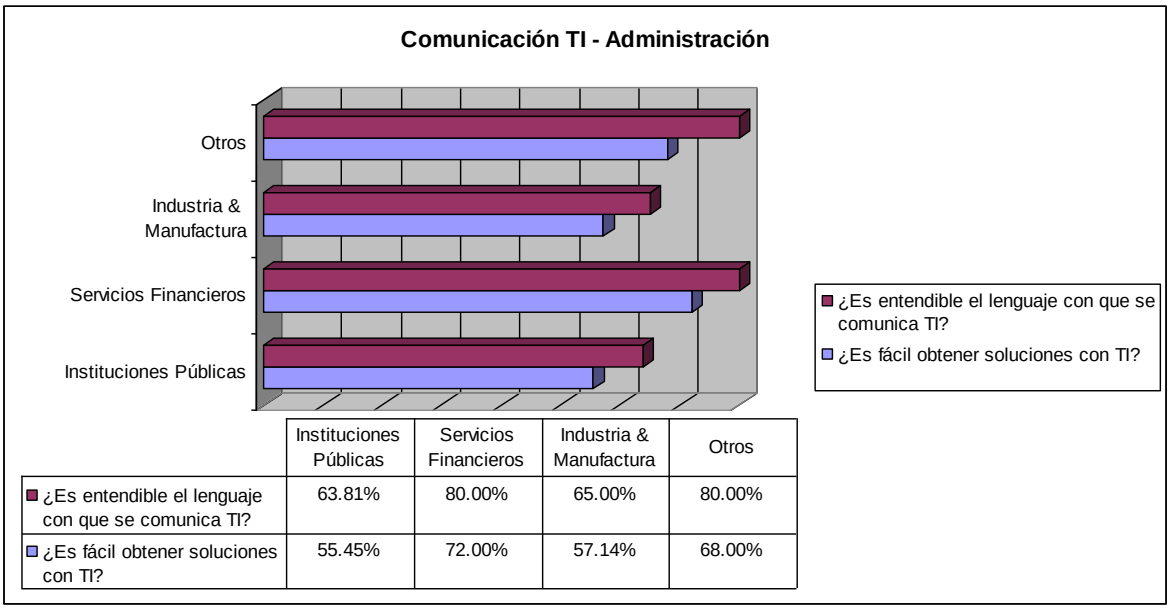
En el sector público y en el sector de industria y manufactura la barrera del lenguaje es más evidente con porcentajes de 63,81% y 65%, respectivamente. El problema en verdad es serio y es de naturaleza global. Tan es así que en el curso SANS Security Leadership Essentials for Managers with Knowledge 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



	Instituciones Públicas	Servicios Financieros	Industria & Manufactura	Otros
¿Es entendible el lenguaje con que se comunica TI?	63.81%	80.00%	65.00%	80.00%
¿Es fácil obtener soluciones con TI?	55.45%	72.00%	57.14%	68.00%

Ilustración 10
Fuente: Ver reconocimientos

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 2

Informáticos y "no informáticos"		
Pregunta	**Informáticos**	**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%**

Tabla 2
Fuente: Ver reconocimientos

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 3

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 TI?	**63,81%**	**80,00%**	**65,00%**	**80,00%**

Tabla 3
Fuente: Ver reconocimientos

Dado que el tema central de esta tesis es el potenciamiento de los problemas de seguridad por problemas de desconexión, en julio 2007 se realizó una investigación adicional para conocer si existe una cultura de seguridad en las organizaciones.

La seguridad es un recurso bastante costoso, y aunque se cuente con pocos recursos estos podrían ser suficientes para crear o al menos intentar crear una cultura aceptable en este sentido.

El primer paso que se debe dar es trabajar en la formulación de políticas adecuadas de seguridad y las normativas asociadas, lo cual es fundamental para saber exactamente cómo y por quién la información se accedió, guardó, transfirió, modificó, se borró, etc., pilar fundamental del término no repudiación o irrebatibilidad que se ha mencionado con anterioridad.

En la formación o creación de toda cultura, juegan un papel importante los fundadores o los primeros miembros de dicha cultura. Por cultura se entiende el conjunto de valores, creencias, rituales, normas, creencias, etc. que posee un determinado grupo de individuos que comparten un espacio determinado. Esto es válido también al llevarse a una organización y se entiende como cultura organizacional. Esta se desarrolla en el tiempo con el aporte de los fundadores de una institución y conforme va creciendo, se enriquece con los aportes también de quienes llegan a ella.

No se habla de culturas buenas o malas aunque sí de culturas fuertes, débiles, dominantes, etc. No se pretende en este trabajo el profundizar en estos aspectos, sólo se tomarán unas características para lograr entender el comportamiento de

una cultura informática, que es una subcultura de una cultura organizacional más amplia.

Es importante resaltar que en una organización pueden subsistir varias culturas, las cuales conforman la cultura general. Esto es así porque aunque compartan valores generales, es altamente probable que en organizaciones de medianas a pequeñas, al producirse la departamentalización, los individuos que conforman una división o departamento comparten valores muy propios. Por ejemplo, un grupo de mecánicos, un grupo de carpinteros, etc. que trabajan en grupos muy especializados y que desarrollan valores que llegan a compartir, se cohesionan y son parte de esa cultura en particular.

Queda claro que los colaboradores (empleados) de una organización son el eje que soportan una cultura, la transmiten y la fortalecen o debilitan. En la creación de una cultura de seguridad dentro de una cultura establecida, los colaboradores son de gran valía para poder crear dicha cultura de seguridad.

La organización debe desarrollar un modelo de inducción tal que capacite a los nuevos colaboradores desde su ingreso a ella. Es muy importante que los nuevos colaboradores conozcan política de seguridad pero aun de más relevancia que la ponga en práctica, mediante la adecuada utilización de la capacitación y el monitoreo o seguimiento continuos. Lo normal es que el colaborador lea la política la primera vez y luego tienda a olvidarla o dejarla en el olvido, típico de lo que se llama “entropía” organizativa, esto es un término aportado por la termodinámica: “todos los sistemas tienden en el tiempo al desorden”. Si las políticas se comunican y se ponen en práctica no solamente minimizan el riesgo de pérdida de los datos sino que podrían eliminar la necesidad potencial por los costos de algunos productos de seguridad.

El recurso de menor costo barato para proteger la información es mantener a los colaboradores responsables de ella. Ahora bien, como ya se ha mencionado, el

elemento humano es quien permite que haya fugas en la información. Constantemente se leen artículos en este sentido en los periódicos especializados

Lo común es que las organizaciones no tengan políticas de seguridad escritas y lo interesante es que crearlas no es ninguna pérdida de tiempo. Hay que recalcar que es importante que la organización identifique cuál es la información más relevante y de esta forma detectar qué políticas van a ayudar a salvaguardar estos datos e implementarlas en forma progresiva. Como parte de esta tesis se realizó esta otra investigación para determinar si en algunas organizaciones de las ya estudiadas, y que estuvieron anuentes a que se realizara esta, existía una cultura de seguridad de la información.

Se escogieron diez empresas y se realizó una observación preliminar de campo, en cada una de ellas, con el p, cómo la protegían etc. y observar también cómo ponían en prácticas algunas medidas de seguridad, aunque no estuvieran escritas. Luego se aplicó un una encuesta para recabar más información.

Este cuestionario, que fue contestado tanto por personal del área de TIC como usuarios en general, es un poco extenso y riguroso por el hecho de que los aspectos de la seguridad en TI son muchos y se deseaba evaluar las siguientes áreas:

- ***Política de Seguridad***
  - Política de Seguridad de la Información

- ***Organización de Seguridad de Información***
  - Organización Interna
  - Acceso de Información por Entes Externos

- ***Manejo de Activos***
  - Responsabilidad de Activos

- Clasificación de Información

- ***Seguridad de Recursos Humanos***
  - Contratación de Personal

- ***Procedimiento Seguridad Individual del Empleado***
  - Procedimiento de Seguridad de Información del empleado

- ***Seguridad Física y Ambiental***
  - Equipo de Seguridad

- ***Administración de Comunicaciones y Operaciones***
  - Operaciones
  - Código Malicioso
  - *Backup o respaldo*
  - Seguridad de Redes
  - Administración de Entrega de Servicio por Terceras Partes
  - Planeamiento de Sistema y Aceptación
  - Manejo de Medios de Almacenamiento
  - Intercambio de Información
  - Servicios de Comercio Electrónico
  - Monitoreo

- ***Control de Acceso***
  - Requerimientos del Negocio para Control de Acceso
  - Administración de Acceso de Usuario
  - Responsabilidades del Usuario
  - Control de Acceso por Red
  - Control de Acceso al Sistema Operativo
  - Control de Acceso a Aplicaciones e Información
  - Computación Móvil y Teletrabajo

- Requerimientos de Seguridad en los Sistemas de Información
- Correcto procesamiento en Telecomunicaciones
- Controles criptográficos
- Seguridad de los Archivos de Sistema
- Seguridad en el proceso de desarrollo y soporte
- Administración de la Vulnerabilidad Técnica

- ***Administración de Incidentes de Riesgo***
  - Reporte de Eventos de Seguridad y Debilidades
  - Administración de los incidentes de seguridad de información y mejoras

- ***Administración de Continuidad del Negocio***
  - Aspecto de Seguridad de información de continuidad del negocio

- ***Cumplimiento***
  - Cumplimiento de Requerimientos Legales
  - Cumplimiento con políticas de Seguridad y Estándares y Cumplimiento Técnico
  - Consideraciones de Auditoría de Sistemas de Información

Hay secciones de este cuestionario que un usuario no puede contestar por diversas razones: puede ser que no conoce cómo está estructurado o no aplica para el área en el que trabaja. Para ello aparece en el formulario los rubros *No hay Información o No Aplica*.

Además para hacer el muestreo de cómo se encuentran en las áreas antes mencionadas se planteó de forma tal que ellos lo pudieran valorar por porcentajes y al final tener un valor que ayudara a detectar la fortaleza o debilidad con que se encuentra cada área de la empresa u organización en estudio.

Se aclaran algunos términos para lograr mayor claridad, otros términos ya se han presentado a lo largo de esta tesis.

Sistema de Gestión de Seguridad

Para tener una buena gestión de seguridad se debe conocer el concepto de ***Calidad***.

> Se entiende como ***calidad*** al conjunto de características inherentes de un producto, proceso o sistema que permiten satisfacer las necesidades y expectativas de los clientes y de otras partes interesadas. [12]

Para entender el concepto ***Sistema de Gestión*** se desglosa en cuatro definiciones para mayor claridad.

- Es un sistema para establecer la política y objetivos de una organización y lograrlos, mediante una estructura organizativa donde las funciones, responsabilidades, autoridad, etc. de las personas, están definidas.

- Son el conjunto de procesos y recursos necesarios para lograr los objetivos.

- Es la metodología de medida y de evaluación para valorar los resultados frente a los objetivos, incluyendo la retroalimentación de resultados para planificar las mejoras del sistema.

- Es un proceso de revisión para asegurar que los problemas se detectan y se corrigen, y las oportunidades de mejora se implementan cuando estén mejoradas.

[12] ISO 9000:2000.

Elementos Comunes de un Sistema de Gestión

Los elementos comunes de un Sistema de Gestión se mostrará en el siguiente gráfico y la explicación de cada uno de ellos se definirá posteriormente.

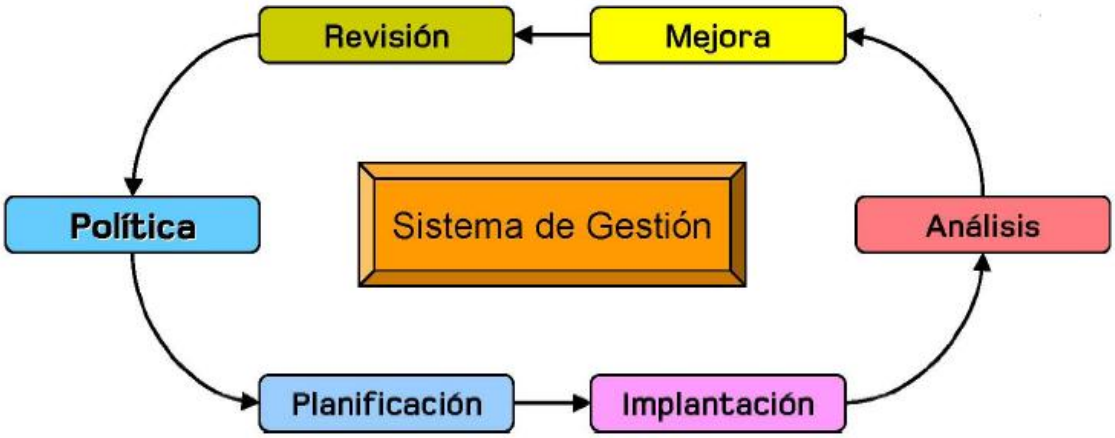


Ilustración 11

Política

Para demostrar el compromiso de la organización con los requisitos del Sistema de Gestión y establecer unos principios y orientación global.

Planificación

- Identificación de necesidades y requisitos.
- Selección de los elementos a ser gestionados.
- Establecimiento de objetivos.
- Identificación de recursos.
- Identificación de la estructura organizativa, funciones, responsabilidades y autoridad.
- Planificación de los procesos operativos.
- Preparación de planes de contingencia para eventos previsibles.

Implantación

- Control de las actividades para lograr los objetivos.
- Gestión de recursos humanos.
- Gestión de otros recursos.
- Documentación y su control.
- Comunicación.
- Relaciones con proveedores y subcontratados.

Análisis

- Monitorización y mediciones.
- Estudio y gestión de no conformidades.
- Auditorías del sistema de gestión.

Mejora

- Acciones preventivas.
- Acciones correctivas.
- Mejora continua.

Revisión

- Para determinar su rendimiento.
- Asegurar su adecuación permanente.
- Asegurar su suficiencia y efectividad.
- Desarrollar mejoras.
- Plantear nuevos objetivos cuándo sea necesario.

En resumen, si una organización quiere implementar un sistema de gestión de la seguridad de la información ¿cómo puede lograrlo?

Debe tenerse en cuenta que hay que planificar, hacer, comprobar y actuar en un sistema de gestión de seguridad de la información donde:

Planificar:

- Se define el alcance del Sistema de Gestión de Seguridad de la Información.
- Se define la política del Sistema de Gestión de Seguridad de la Información.
- Se identifican los riesgos.
- Se gestionan los riesgos.

Hacer:

- Define e implanta plan de gestión de riesgos.
- Implanta controles seleccionados y sus indicadores.
- Implanta el Sistema de Gestión.

Comprobar:

- Desarrolla procedimientos de monitorización.
- Revisa regularmente el Sistema de Gestión de Seguridad de la Información.
- Revisa los niveles de riesgo.
- Audita internamente el Sistema de Gestión de Seguridad de la Información.

Actuar:

- Implanta las mejoras.
- Adopta acciones preventivas y correctivas.
- Comunican acciones y resultados.
- Verifica que las mejoras cumplan con su objetivo.

Ilustración 12

Se analizó cómo se encuentra valorado este concepto en las organizaciones escogidas, las cuales constituyeron la muestra: una universidad pública (sector educación), tres entidades bancarias (financiero), tres de servicios, cinco de industria y tres del sector público. Algunos gráficos no se comentarán pues se explican por sí mismos.

El siguiente gráfico muestra qué población fue del área de Informática y quiénes eran ajenos a ella:

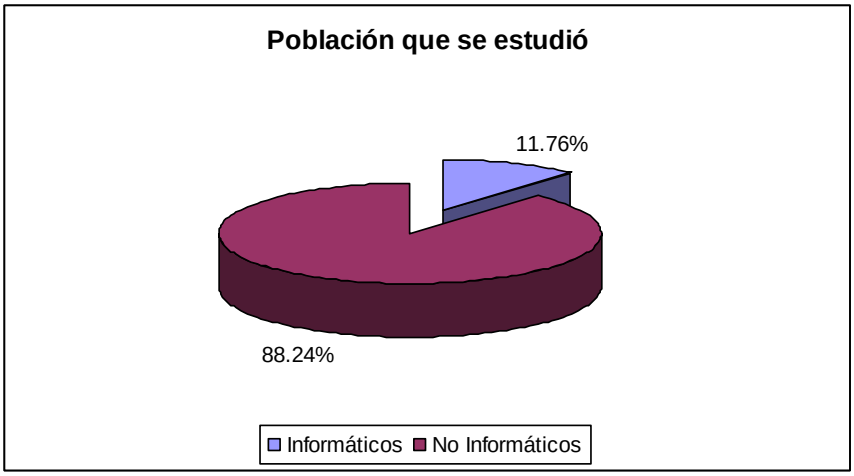


Ilustración 13

En cuanto a los resultados obtenidos se resaltan las preguntas claves que determinaron –en un porcentaje- la realidad que viven esas organizaciones con respecto a la seguridad.

¿Existe una política de seguridad de la información aprobada por la gerencia, publicada y comunicada adecuadamente a todos los colaboradores?

En el gráfico se encuentra la respuesta a esta pregunta. El 65% indica un cumplimiento completo o mayor mientras que un 35% indica que no tienen políticas establecidas o bien publicadas. Es interesante que los entrevistados del sector industrial manifiestan tener políticas de seguridad. Esta no es la tónica, pero si se contrasta con la investigación original de desconexión, realizado en otro momento, hay consistencia. En la universidad pública manifiestan tener políticas de seguridad aunque en otro momento expresan no tener un comité de informática.

Por supuesto que, dado que las organizaciones donde se aplicó el instrumento son pocas y son tan solo una muestra pequeña de la muestra original, no se puede concluir que este sea el comportamiento general de todos los sectores encuestados, pero da una idea de la importancia relativa que se le da al aseguramiento de la información en dichas organizaciones. Se agrupan los datos

solo por razones de tener una idea general, aunque lo importante es el análisis de cada organización o mejor aún, por sector. Por limitaciones de tiempo sólo se trabajo con esta muestra de tamaño reducido.

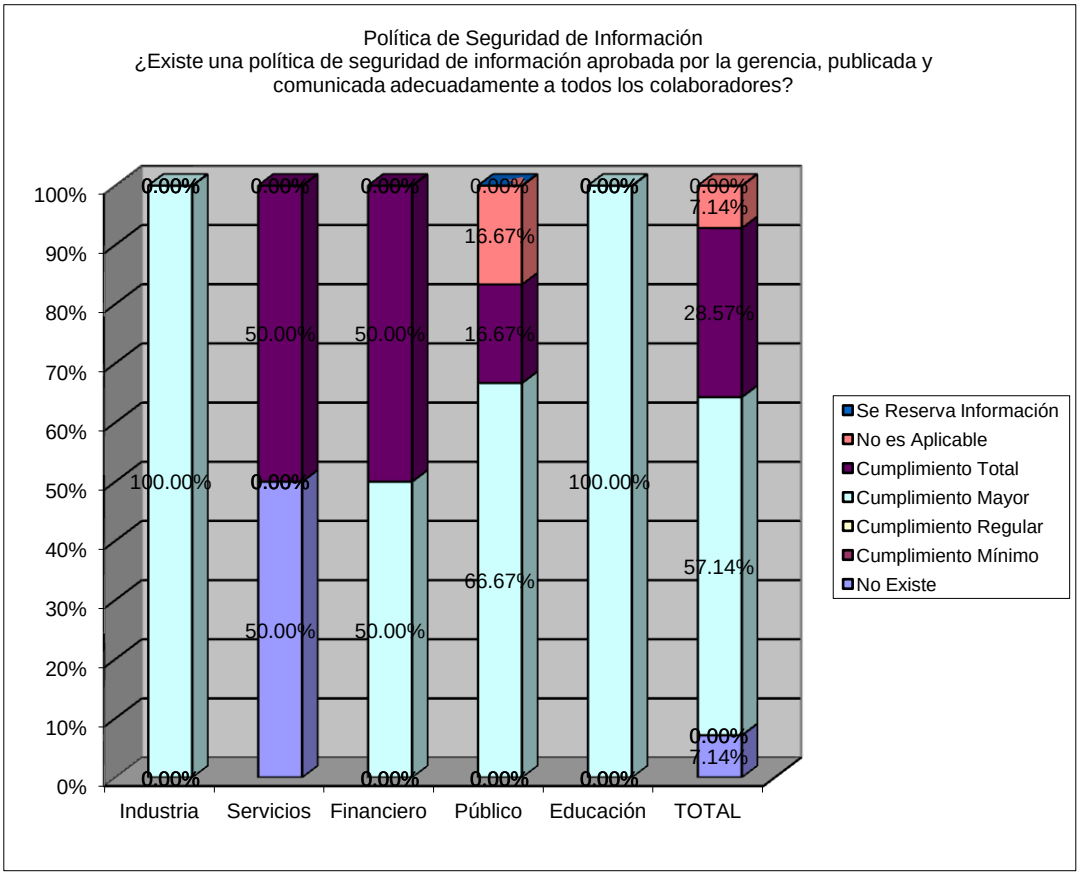


Ilustración 14

Este gráfico que sigue es interesante también.

Los entrevistados sienten que existe un apoyo bajo en temas relativos a la seguridad, se sesga por tener solo una institución del sector educación que en apariencia si recibe ese apoyo en temas de seguridad. Lo mismo sucede con el sector industrial.

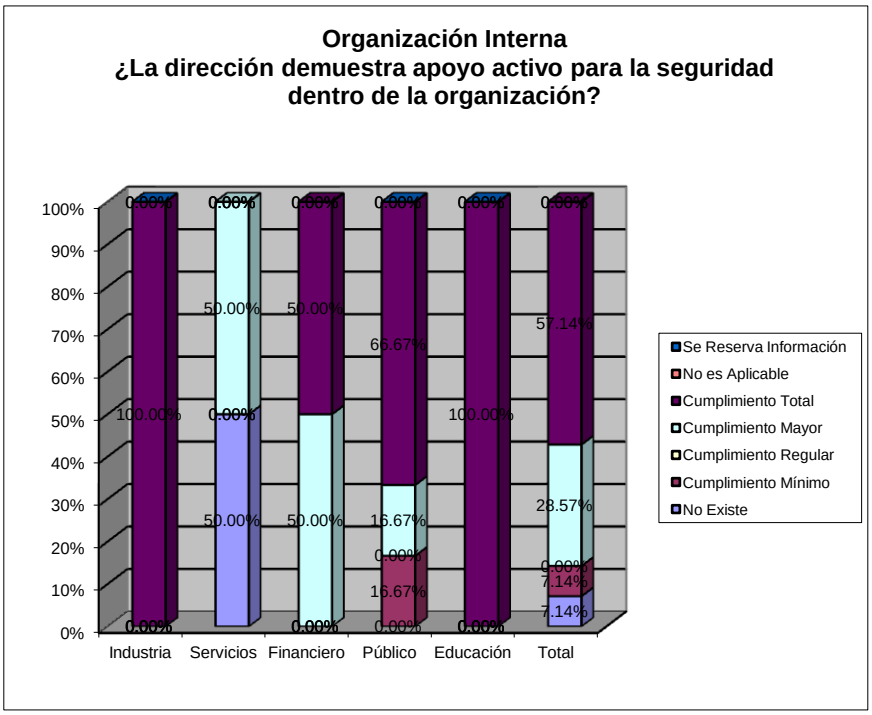


Ilustración 15

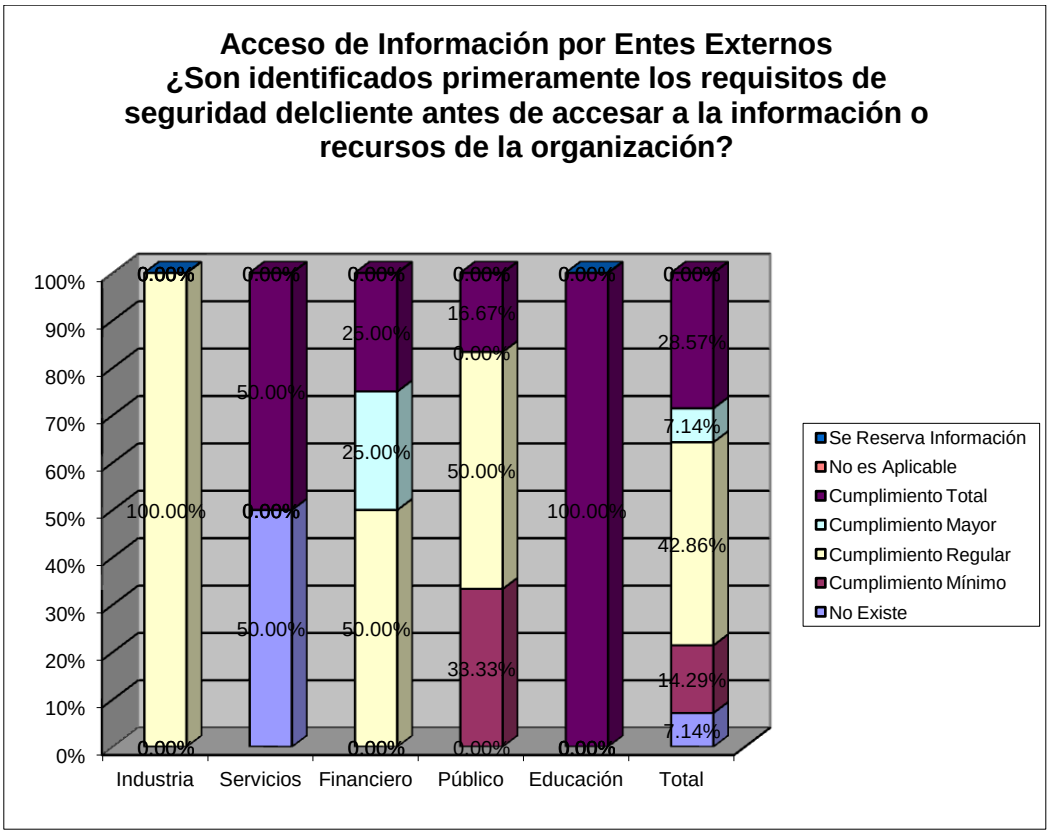


Ilustración 16

Esta gráfica muestra que este aspecto también es deficiente; solo un 35% está en rango cumplimiento mayoritario a total, la mayor parte está en el rango de regular

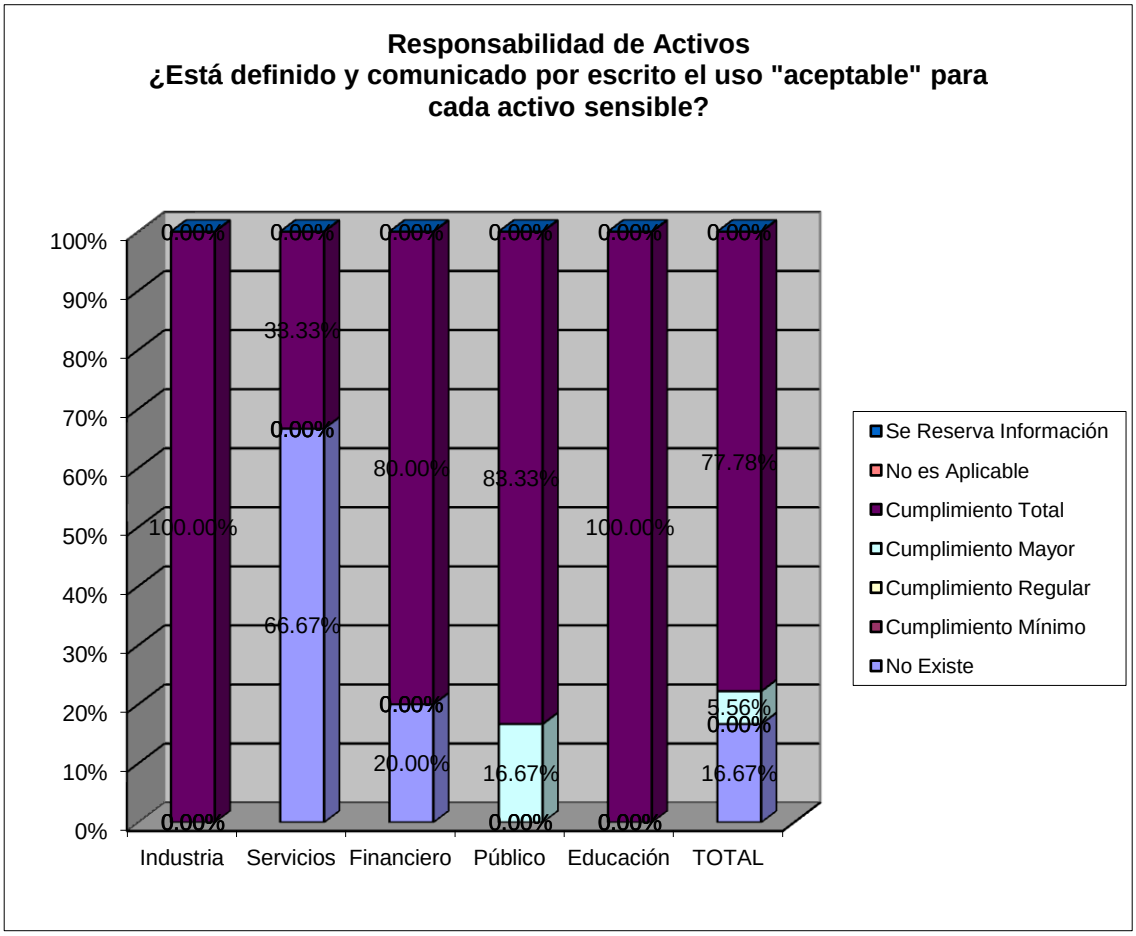


Ilustración 17

En cuanto manejo de activos es una de las áreas más débiles en las organizaciones observadas, un 86% indica cumplimiento mínimo o simplemente no existe.

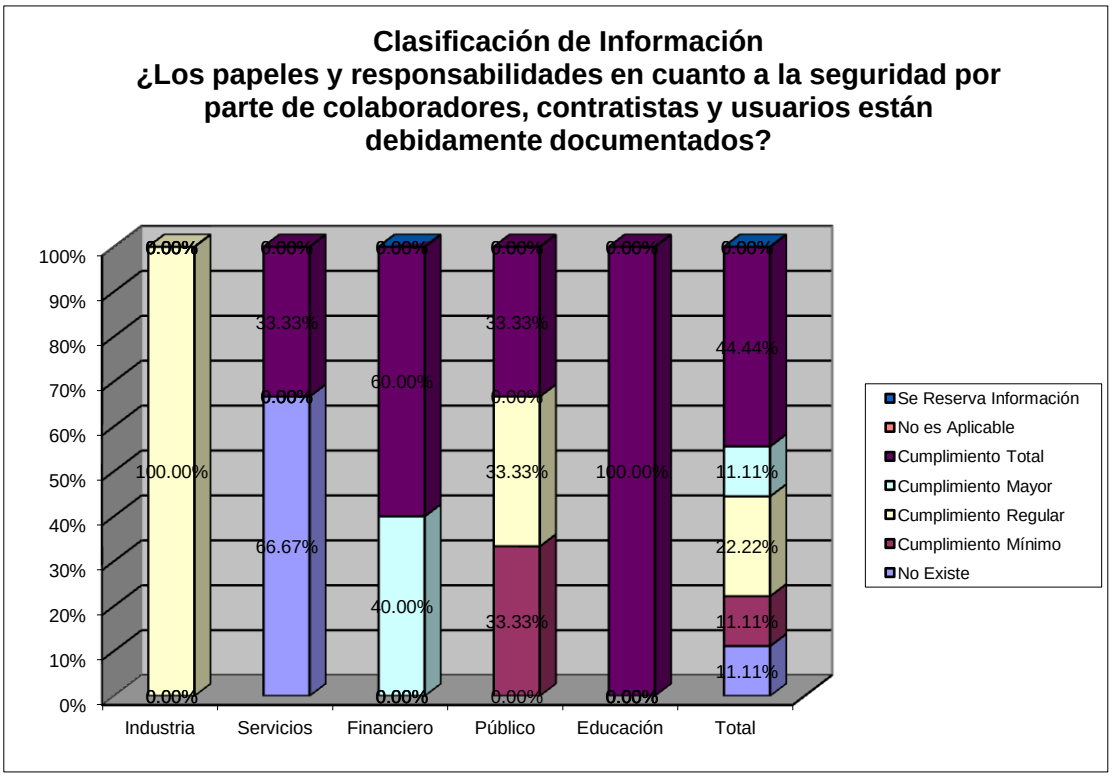


Ilustración 18

El aspecto de la comunicación de papeles y responsabilidades varía según el sector. Lo importante de resaltar es que no en todas las organizaciones se le da la importancia que se merece a la asignación de las responsabilidades inherentes al aspecto de seguridad. De hecho ya se ha resaltado que el problema de los *insiders* puede convertirse en el problema más serio de las organizaciones.

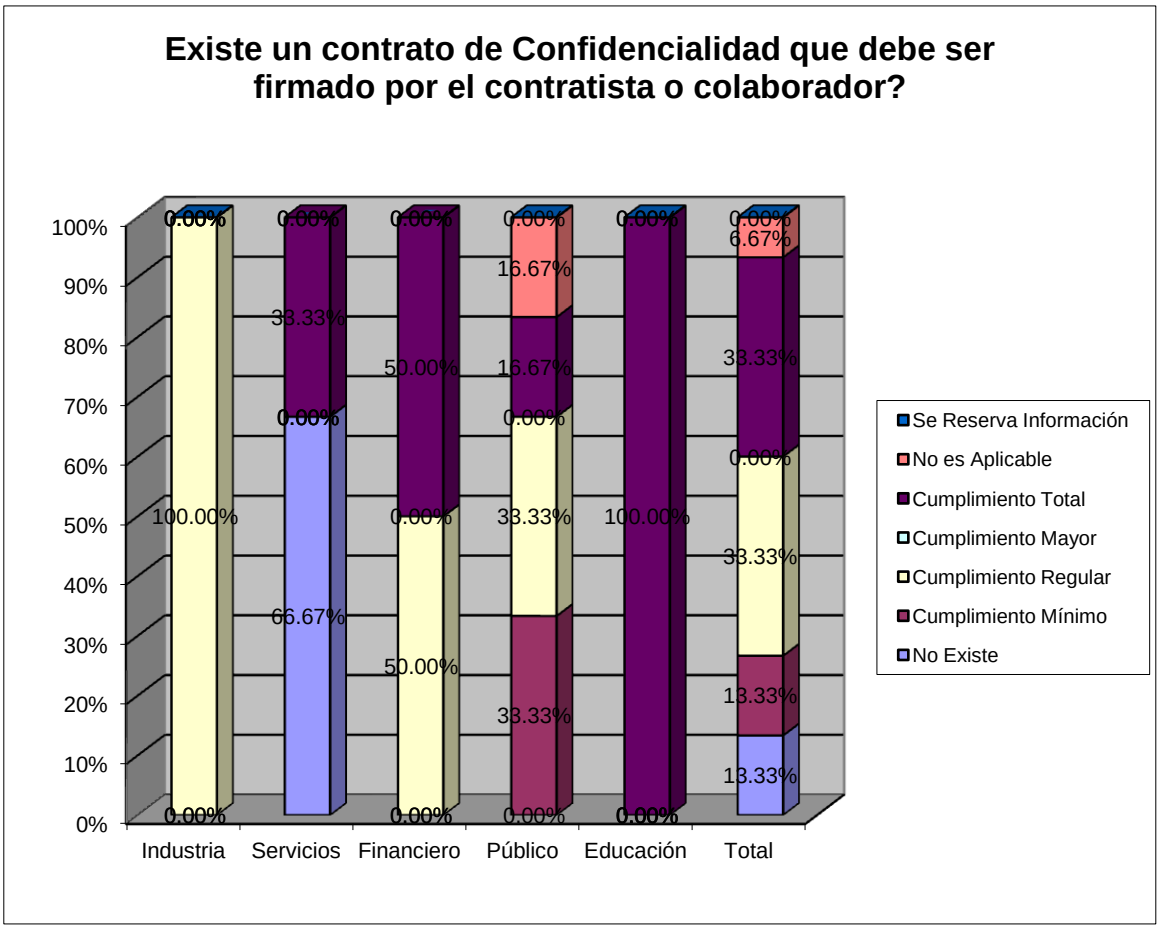


Ilustración 19

Una de las debilidades que se manifiestan en las organizaciones es que rara vez el personal contratado firma un acuerdo de confidencialidad. Aunque en el caso de educación e industria manifiestan que si lo firman, al investigar con otros colaboradores de dichos sectores, estos manifestaron que no es así, que sólo en ciertos casos. Dadas las respuestas que se obtienen en el sector Industria y en el de la Universidad, se cree que se está frente a información no válida.

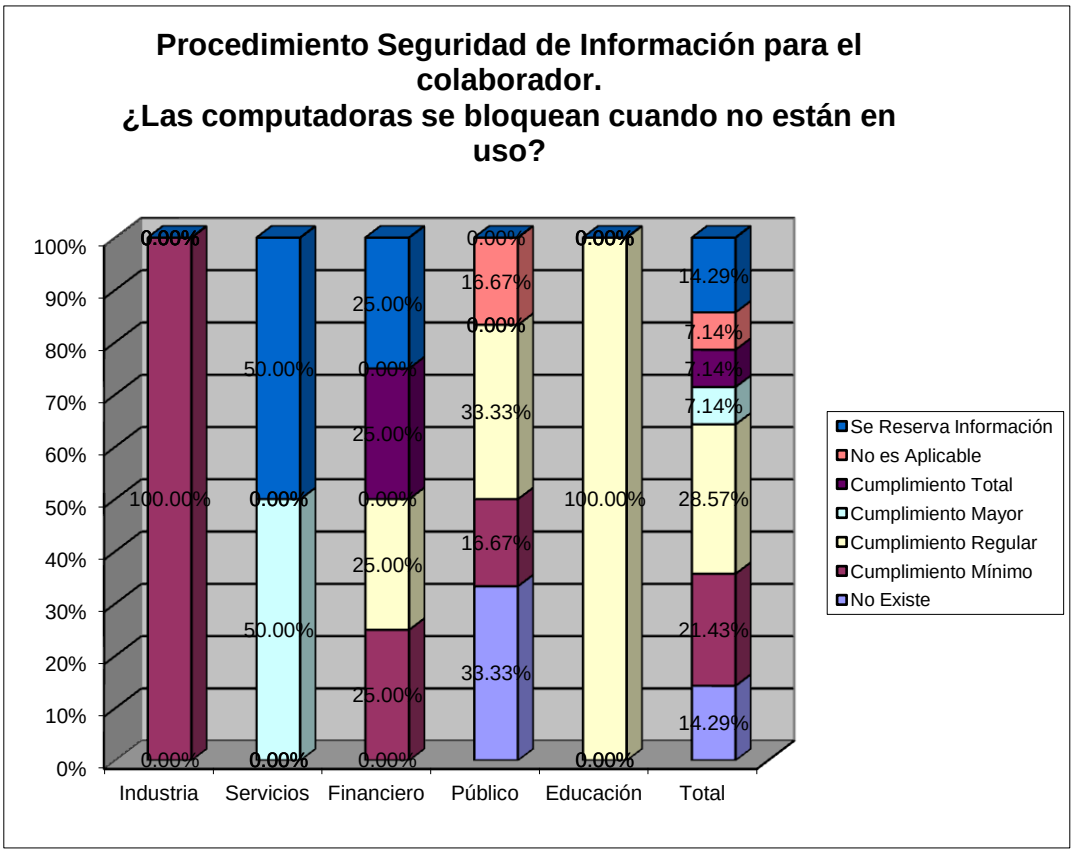


Ilustración 20

Por regla general las personas cuando se levantan de sus lugares de trabajo o estudio, rara vez cierran las sesiones abiertas en sus computadores. Esto conlleva un problema serio de seguridad, no solo para la información propia del individuo sino para la de una organización si ésta está en red de área local o conectada a servidores centrales. Es relativamente sencillo y rápido el grabar información en dispositivos tipo USB (*Universal Serial Bus*, memorias rápidas) o bien mandar información por medio de un correo electrónico. Más grave aún, si no se ha cerrado la sesión y se interactúa con un servidor, acceder la información sin necesidad de registro y autenticación, pues el usuario que dejó la sesión abierta ya se había autenticado.

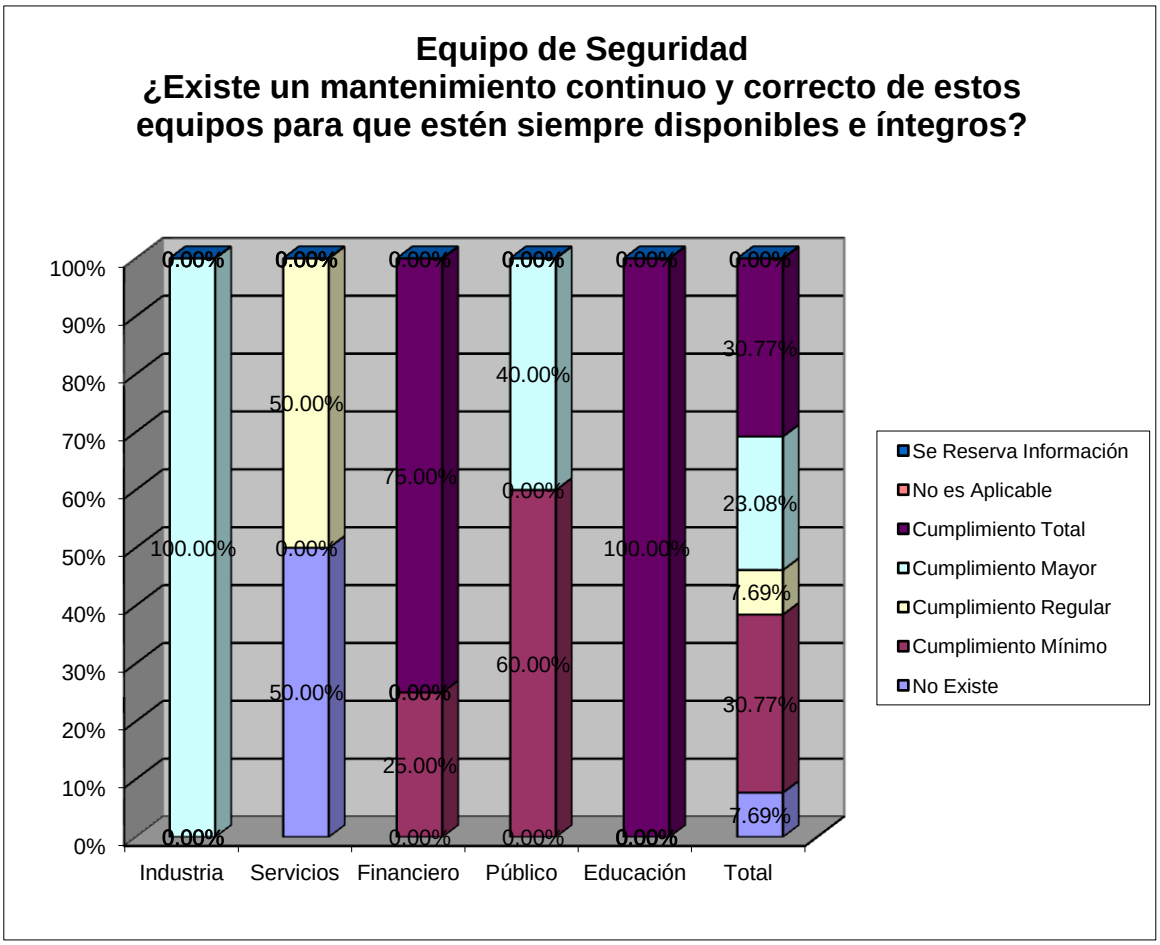


Ilustración 21

Excepto por los sectores ya mencionados, Industria y Educación, en la mayoría de las respuestas obtenidas, en todas las preguntas, no se encontrarán valores al 100%, excepto en la pregunta donde se indica si hay respaldos a la información o no. Todo esto refleja el problema de desconexión existente en las organizaciones y que nada tiene que ver con alineamiento de las tecnologías.

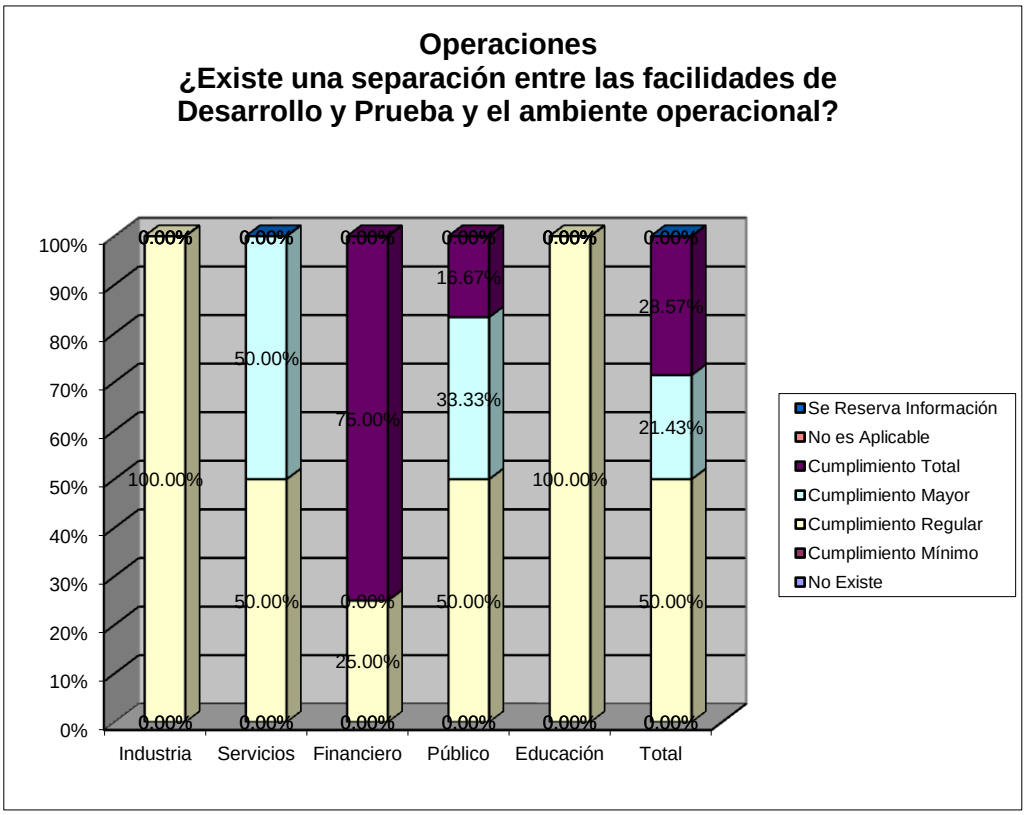


Ilustración 22

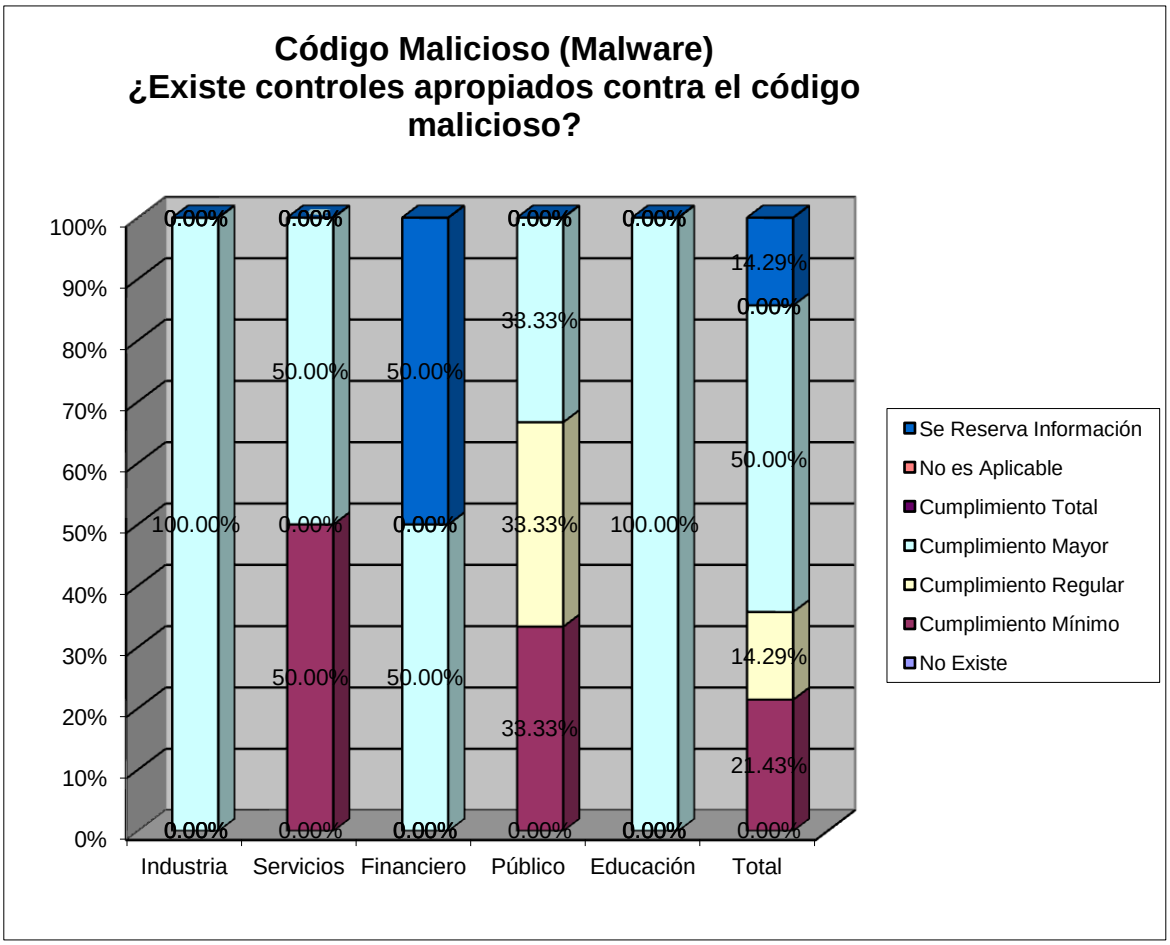


Ilustración 23

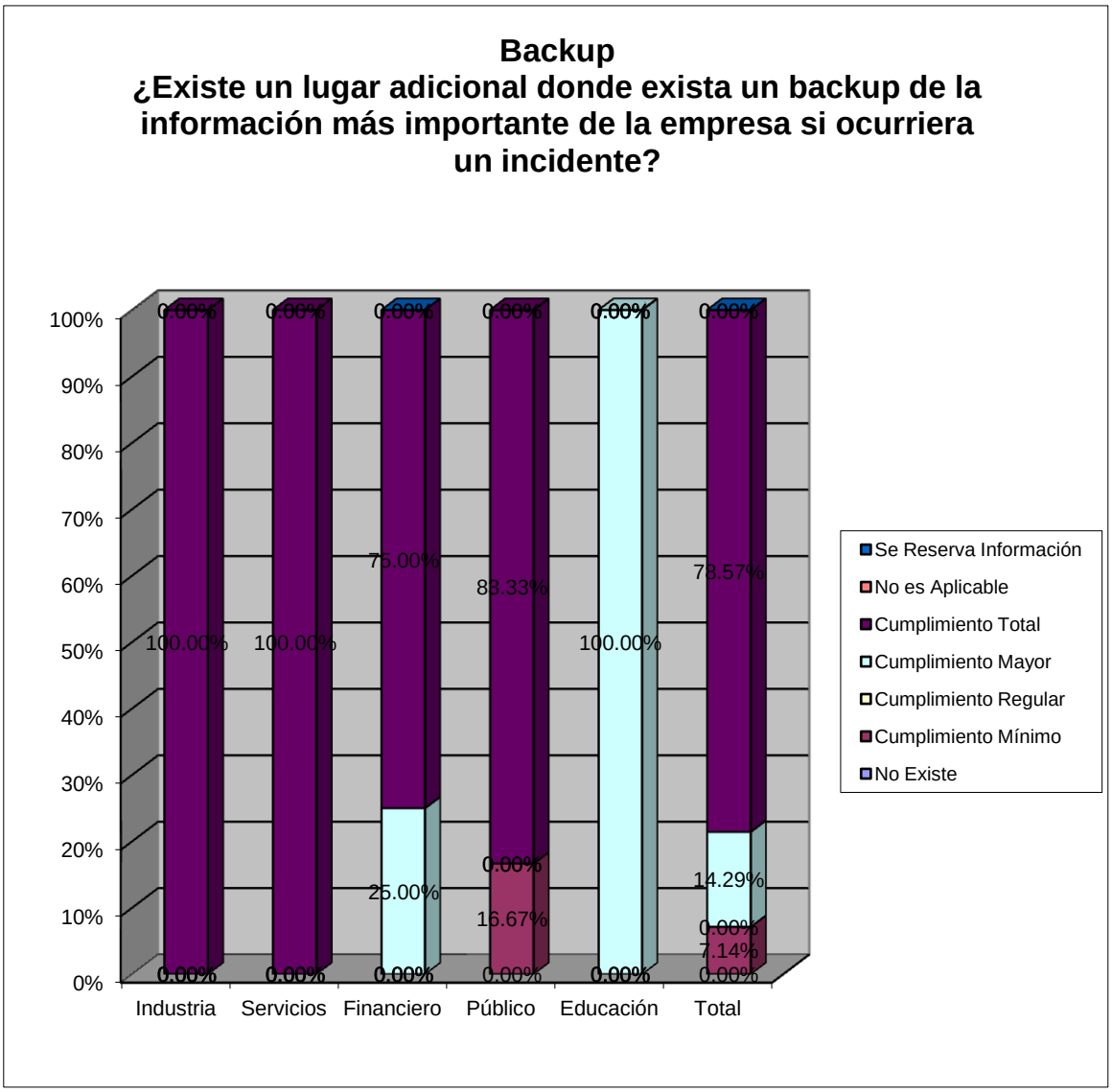


Ilustración 24

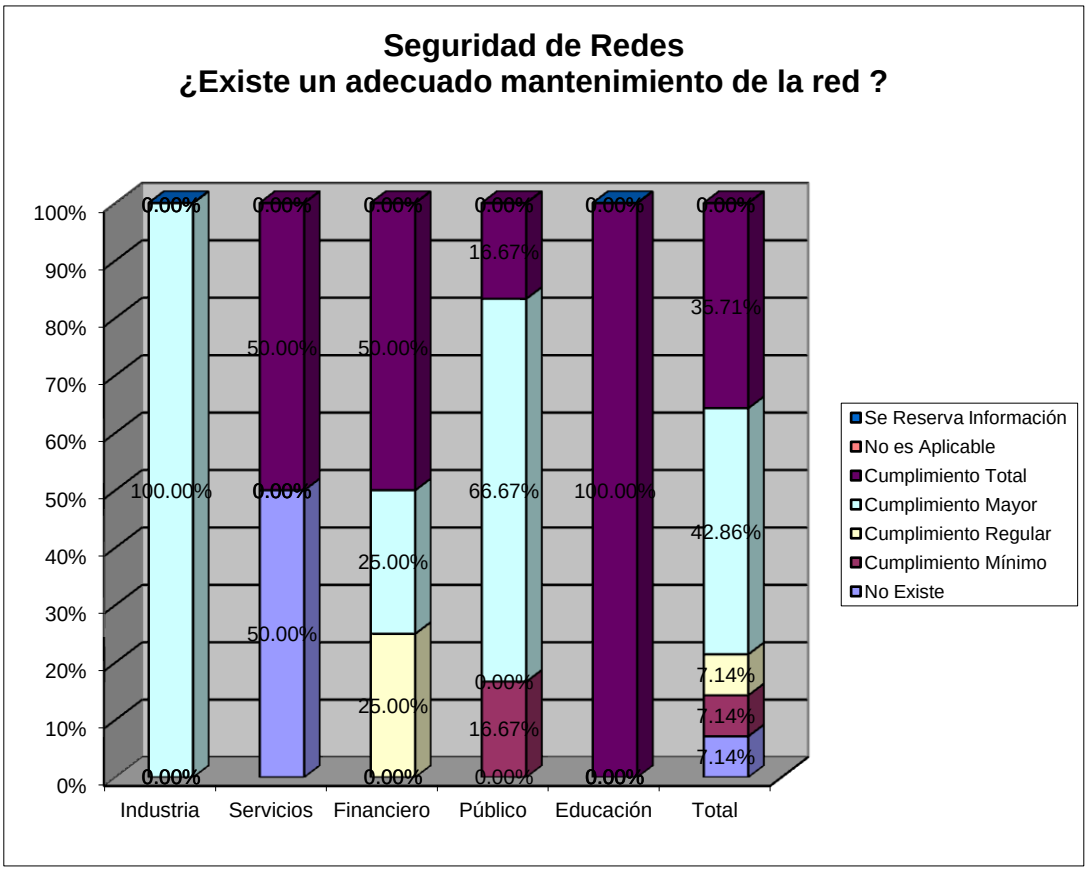


Ilustración 25

Este es otro de las preguntas donde hubo mayor acuerdo, casi en su totalidad indicaron un cumplimiento satisfactorio, lo cual es normal porque se trata de un asunto de capa tres, para lo cual existen normativas estándar.

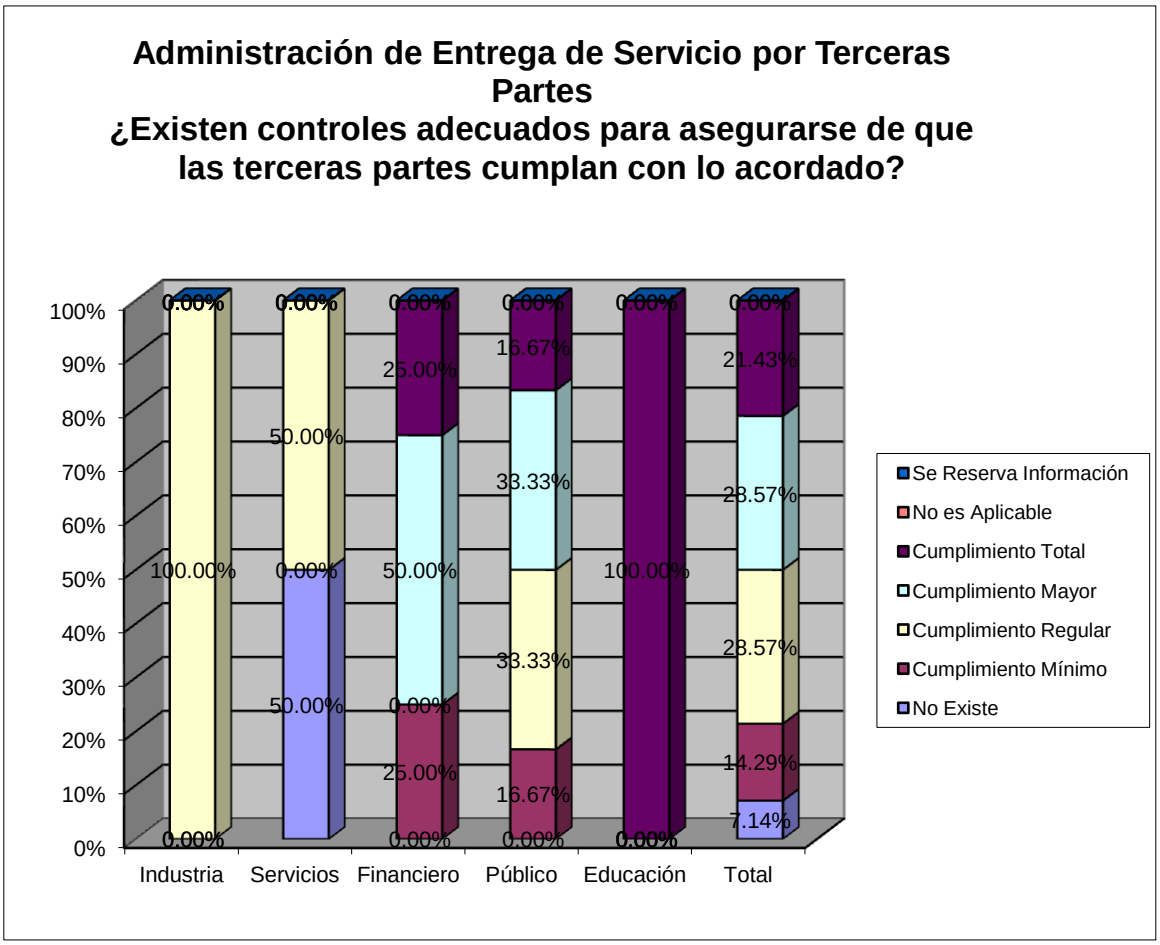


Ilustración 26

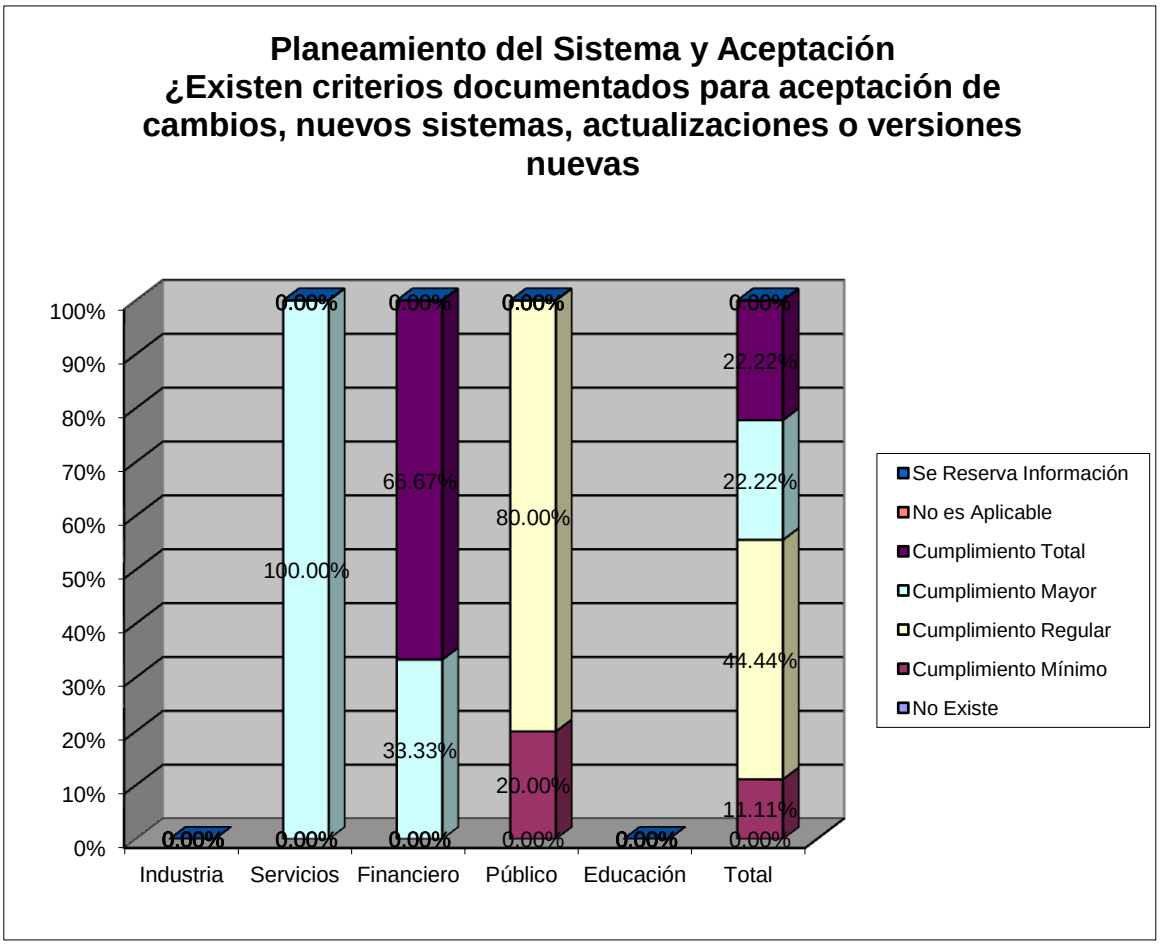


Ilustración 27

Una de las debilidades mayores en la Ingeniería de Sistemas, es el de documentar los cambios a las aplicaciones. Generalmente se realizan las modificaciones, pero estas no quedan registradas en una bitácora. Pasado un tiempo, ya nadie recuerda por qué se dio el cambio quién la realizó. Si se hace, no es porque haya, en la mayoría de los casos, una política expresa y menos asociada con las de seguridad.

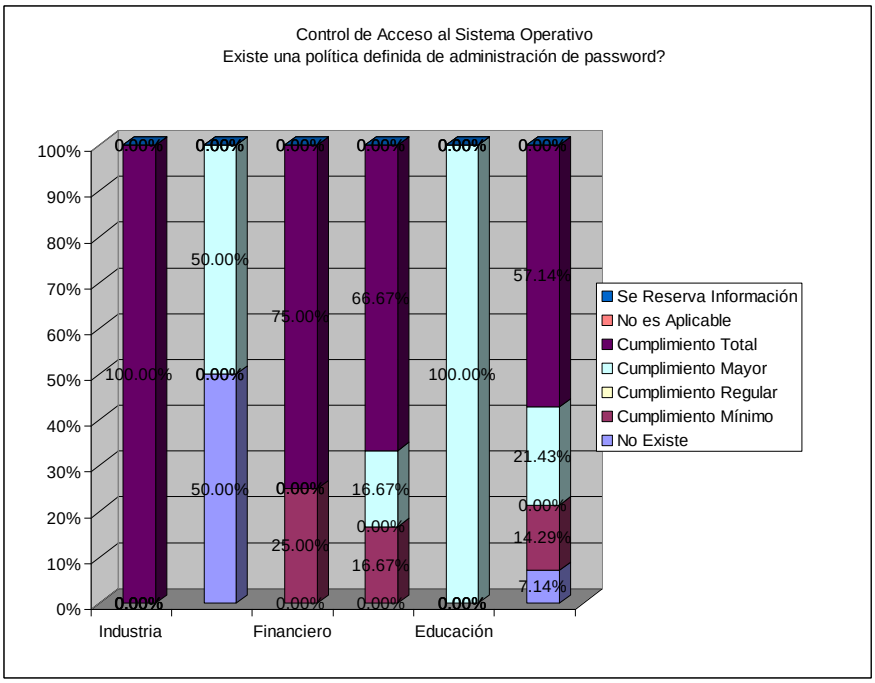


Ilustración 28

La mayoría de las organizaciones simplemente realizan las actualizaciones de los sistemas operativos y rara vez verifican que los cambios no produzcan efectos adversos, dan por sentado que las actualizaciones eran correctas y que también quedaron correctamente instaladas.

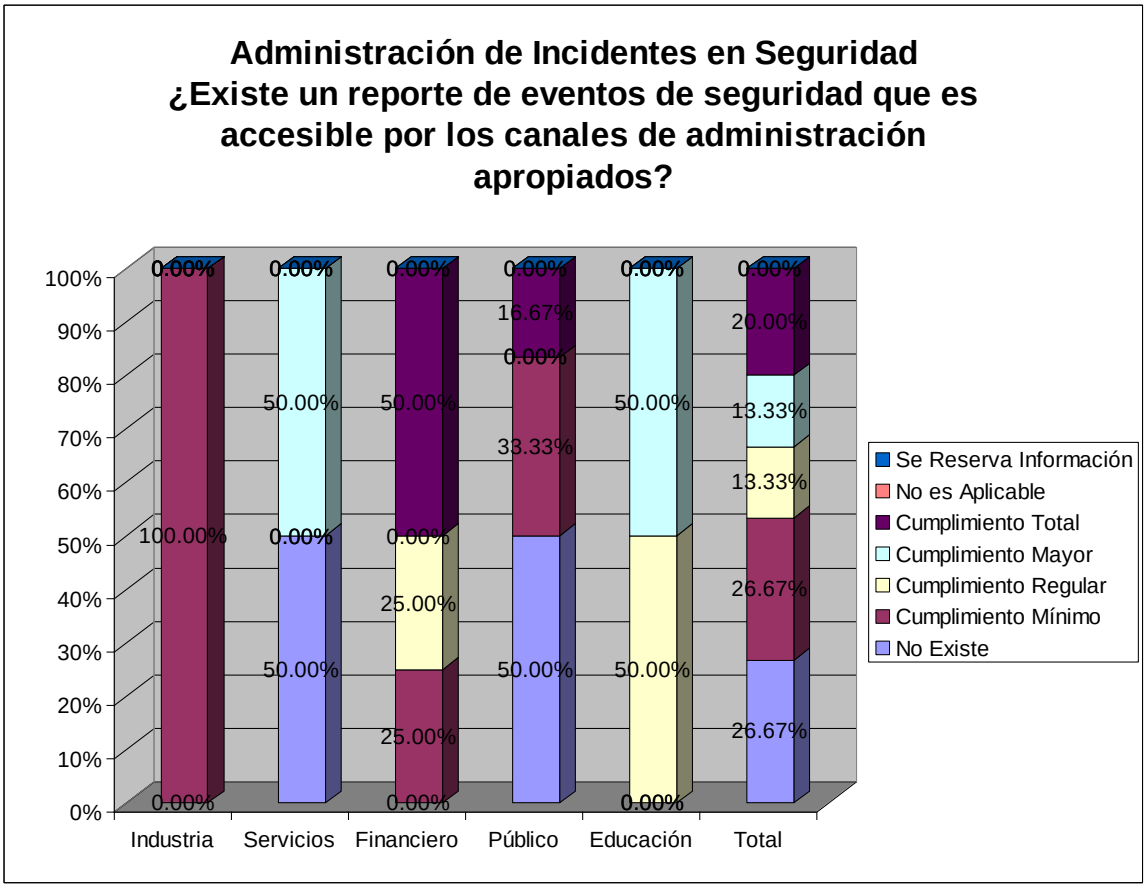


Ilustración 29

Todos los sistemas de detección de intrusos, los enrutadores y los cortafuegos, por citar algunos de los elementos de la defensa en profundidad, generan gran cantidad de información. Precisamente por ser de gran volumen, son dejados de lado por quienes deberían revisarlos continuamente. Es probable que algunos hayan contestado a esta pregunta desconociendo que en realidad sí cuentan con esas bitácoras; sin embargo, de nada sirven si nadie las analiza.

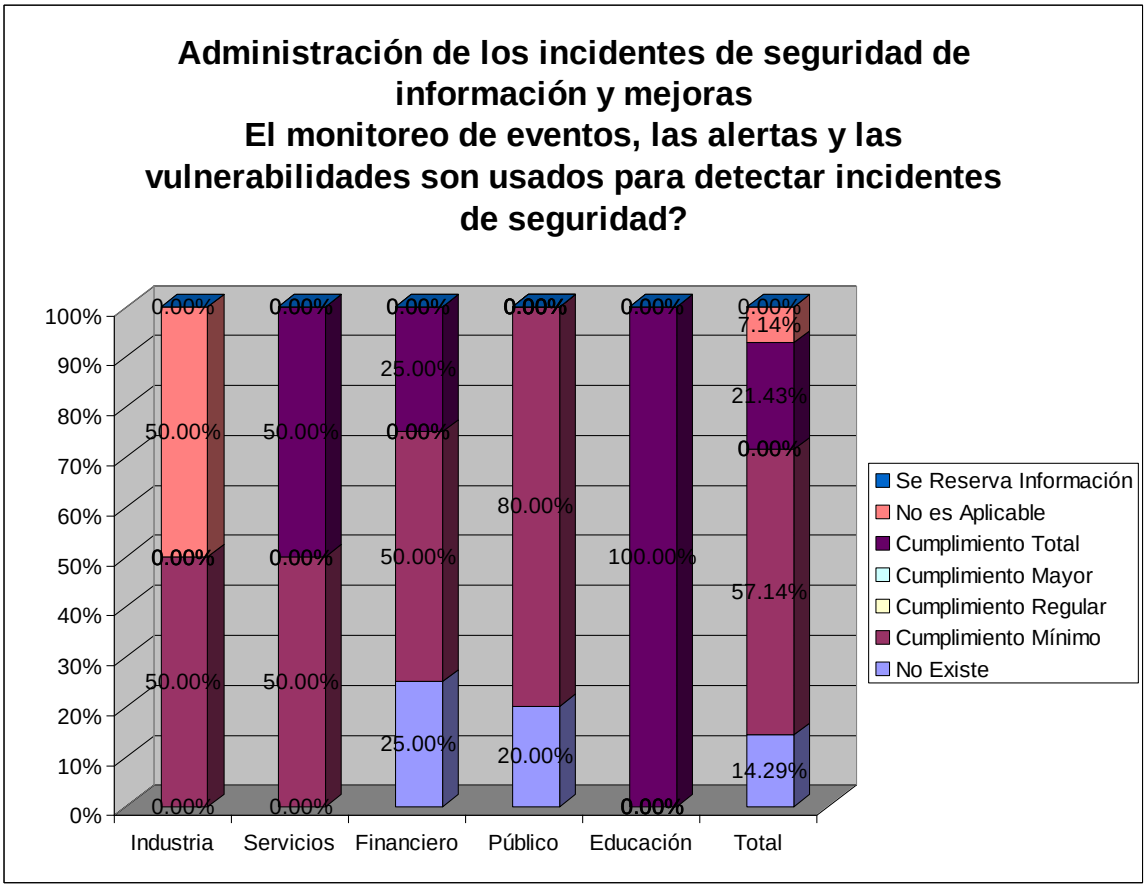


Ilustración 30

La debilidad manifiesta, aún en esta pequeña muestra, es que la información generada por las aplicaciones de seguridad, tal como se mencionó en el anterior gráfico, no se utiliza para analizar incidentes de seguridad. Por lo tanto, todo lo anterior refleja una cultura de seguridad incipiente. No es necesario efectuar grandes análisis ni tomar mayores muestras, dado que los ataques que sufre la información y los ataques que van dirigidos incluso a los activos de las personas, son reflejo claro de ausencia de medidas adecuadas de aseguramiento de la información.

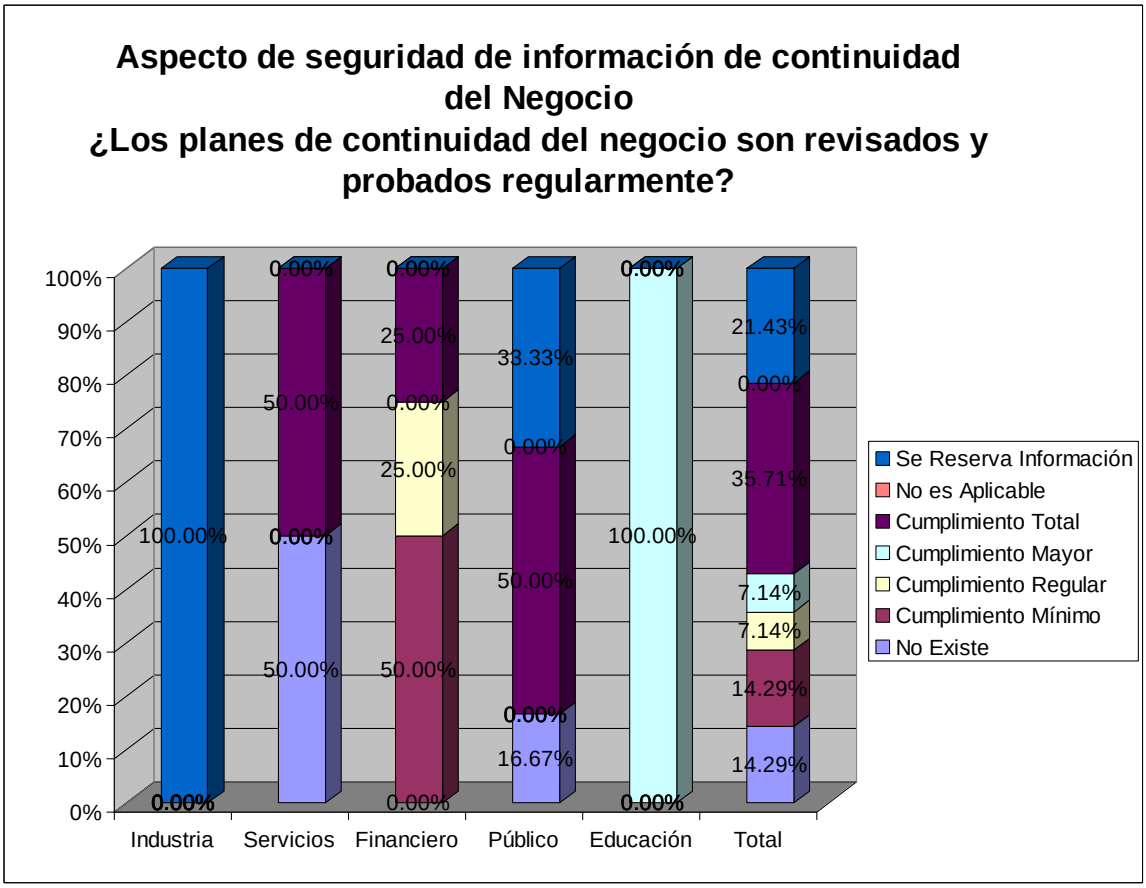


Ilustración 31

Si no existen políticas de seguridad, menos existirán políticas para la continuidad de los negocios. En las empresas muy estructuradas, de gran tamaño, de diferentes sectores es normal encontrar políticas en este sentido, no así en las empresas de medianas a pequeñas.

La razón es muy sencilla: costo. Si se tiene la idea que las TIC brindan pocas ventajas competitivas o si bien si no se tiene claro su papel dentro de la actividad del giro del negocio, menos se invertirá en un aspecto que es por mucho hasta desconocido.

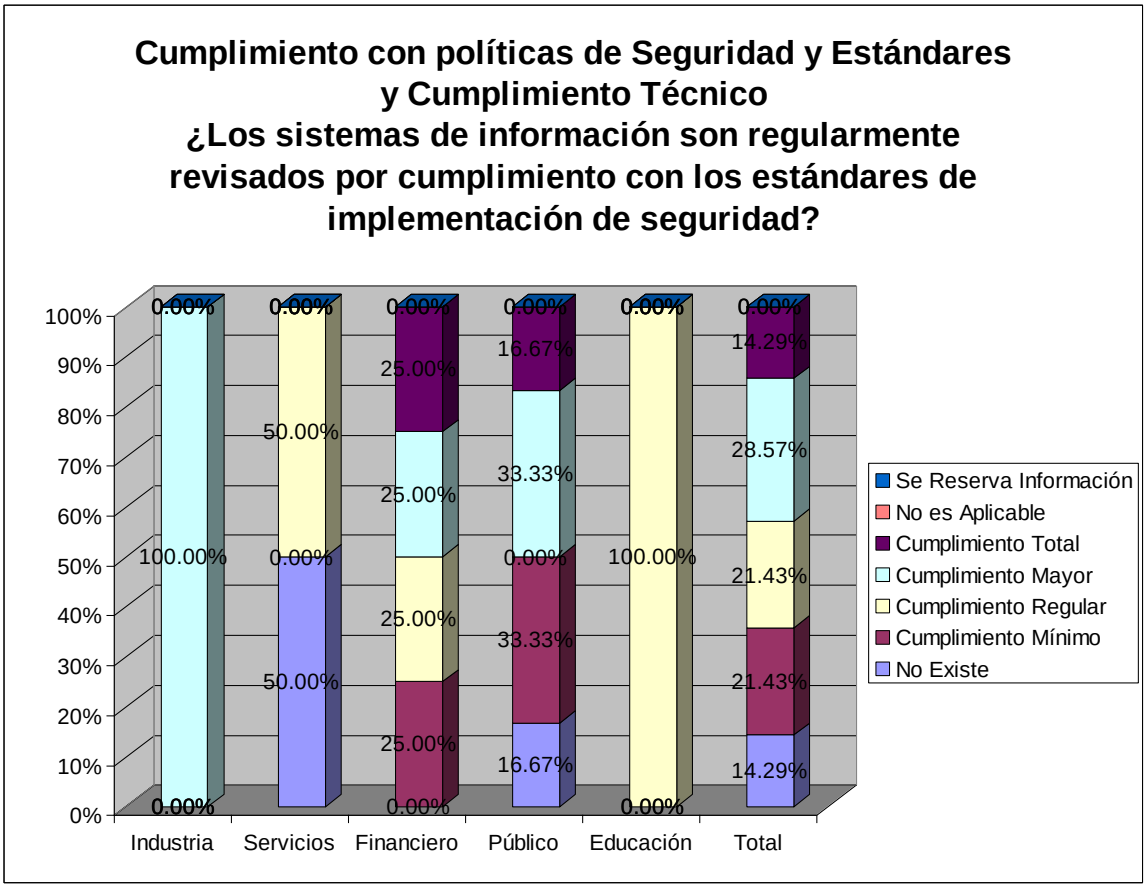


Ilustración 32

Con toda la información recabada, queda muy claro que el fenómeno de la desconexión es real, pero que no es solo entonces un problema de no alineamiento, es un problema que involucra una gran cantidad de variables.

En el marco de esta tesis y de acuerdo a la investigación de indicadores de desconexión, se detectó que en muchas instituciones los comités de informática no tienen el "peso" que debieran en sus organizaciones o bien sus decisiones no son vinculantes. Se decidió entonces analizar qué papel desempeñan en algunas instituciones y también el trabajar con un grupo de ellas que dada su naturaleza educativa, debieran tener comités y no sólo eso, que estos debieran tener un papel preponderante. Por esta razón se escogieron las universidades públicas y privadas de Costa Rica.

El objetivo general que se planteó fue el de estudiar y analizar los comités de tecnologías de información y comunicación en el sector de educación superior de Costa Rica, con la finalidad de poder determinar su importancia dentro de las decisiones estratégicas de los Consejos Universitarios o Juntas Directivas.

Los objetivos específicos fueron:

1. Analizar los comités o grupos de tecnologías de información y comunicación en el sector de educación superior.

2. Indagar sobre la ubicación de los comités de TI en la estructura organizacional.

3. Investigar la composición de los comités de TI en el sector de educación superior.

4. Estudiar la cartera de proyectos de los comités de TI en el sector de educación superior.

    - Evaluar la concordancia entre el plan estratégico institucional y el plan estratégico de los comités de TI.

    - Comparar los comités de TI de las instituciones públicas con los comités de las instituciones privadas.

Para alcanzar los objetivos de esta investigación se trabajó con dos poblaciones diferentes. La primera población de estudio estuvo formada por las cuatro universidades estatales. La segunda población se compuso por las cincuenta y siete universidades privadas autorizadas y reconocidas por el Consejo Nacional de Educación Superior –CONESUP- de Costa Rica.

Para ambas poblaciones se definió la unidad de estudio como los Departamentos de Tecnologías de Información, Unidades de Cómputo o Centros de Cómputo de las universidades.

El marco muestral de esta investigación estuvo compuesta por dos poblaciones finitas, una compuesta por universidades estatales y otra compuesta por universidades privadas. La primera la constituyó las cuatro universidades estatales: Universidad de Costa Rica, Instituto Tecnológico de Costa Rica, Universidad Nacional y Universidad Estatal a Distancia, por lo tanto se realizó un censo. Para la segunda población finita el marco muestral se obtuvo en la página WEB del Ministerio de Educación Pública y lo conformaron todas las universidades privadas autorizadas y reconocidas por este Ministerio al 13 de diciembre del 2006.

Para definir un tamaño representativo de la muestra con respecto a la población universidades privadas, se utilizaron los siguientes parámetros:

Población total	N = 51*
Nivel de confianza	alfa = 0.90
Posibilidad de aceptación	p = 0.50
Posibilidad de rechazo	q = 0.50
Error máximo permisible	E = 0.10

Tabla 4

Una vez que se determinó el tamaño de la muestra, se aplicó el factor de corrección para poblaciones finitas.

Se obtuvo una muestra de 29 universidades privadas y para su escogencia se utilizó el muestreo sistemático, simple, y sin reemplazo.

Con base en los datos originales se procedió a eliminar las universidades que no brindaron información, entre ellas 1 pública, quedando solo para el análisis 3 universidades públicas y 19 privadas, en total 22 universidades y 9 preguntas.

A continuación el análisis de la información solicitada en cada una de las preguntas de la encuesta.

1. ¿Dónde se ubica el departamento de TI dentro de la estructura organizacional?

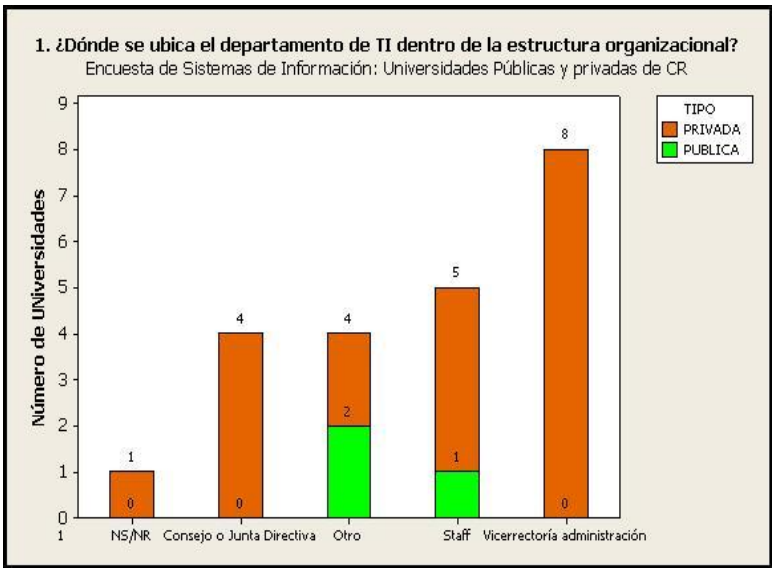


Ilustración 33

A esta pregunta 5 universidades contestaron que los TI son parte del staff de la universidad, incluyendo a una universidad pública, 8 que el departamento de las TIC se encuentra bajo la responsabilidad de la Vicerrectoría de Administración, 4 que están dentro de una opción diferente a las planteadas, incluyendo a 2 universidades públicas y 1 no responde.

2. ¿Existe un Comité de Tecnologías de Información y Comunicaciones en la institución?

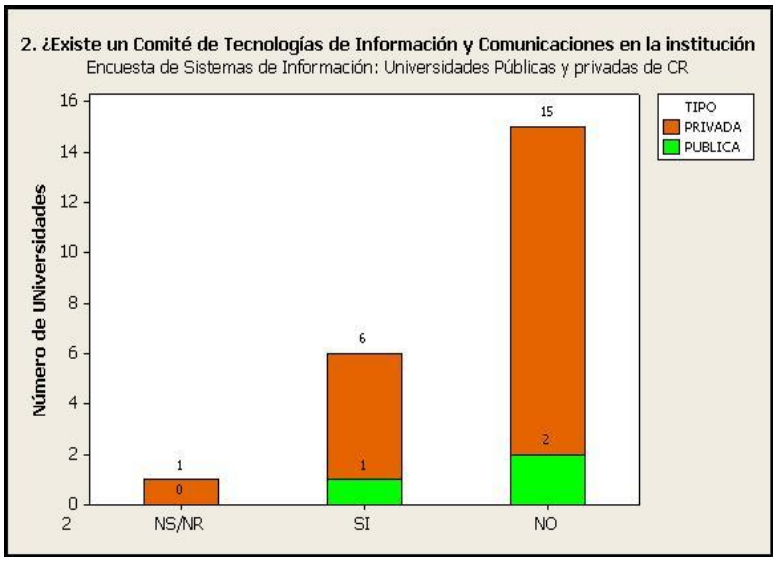


Ilustración 34

A esta pregunta únicamente 6 universidades contestaron que sí tienen comités TIC (un 27%), incluyendo a una pública, el resto que no y 1 no respondió.

3. ¿Quiénes conforman el comité de TIC?

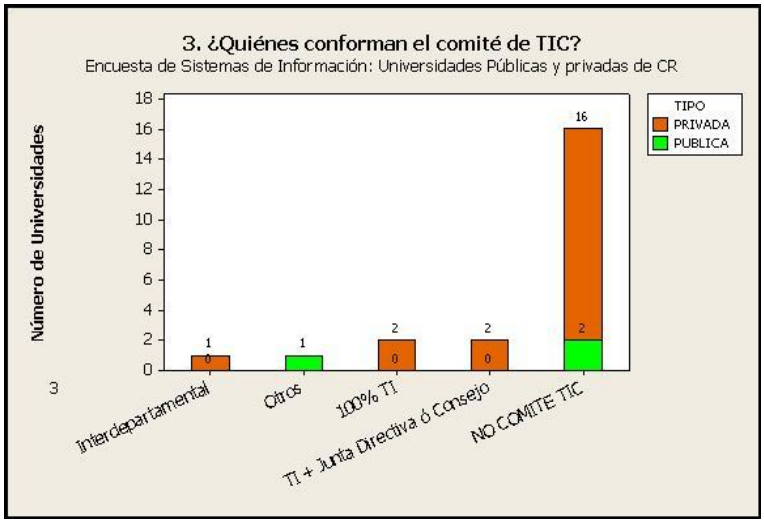


Ilustración 35

El comité de las TIC en las 6 Universidades que respondieron afirmativamente, lo conforman **varios departamentos** en 1 universidad, **100% personal de TIC** en 2 Universidades y **personal de TIC más Junta Directiva o Consejo** en otras 2 Universidades y 1 pública expresa otra alternativa diferente a las solicitadas.

4. ¿Están ligados los objetivos del comité de TIC con los objetivos y planes institucionales?

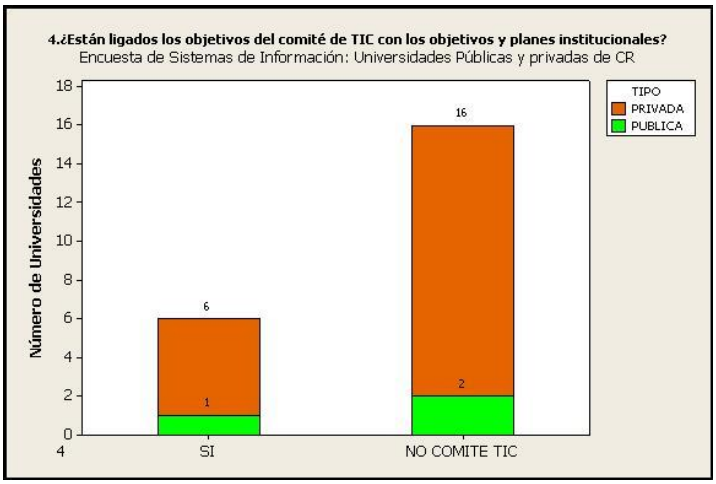


Ilustración 36

Para las mismas 6 Universidades que respondieron afirmativamente, todas mencionaron que los objetivos del comité y los objetivos de los planes de la institución están alineados.

5. ¿Quiénes definen los objetivos de desarrollo e inversión relacionados con el área de tecnologías de información?

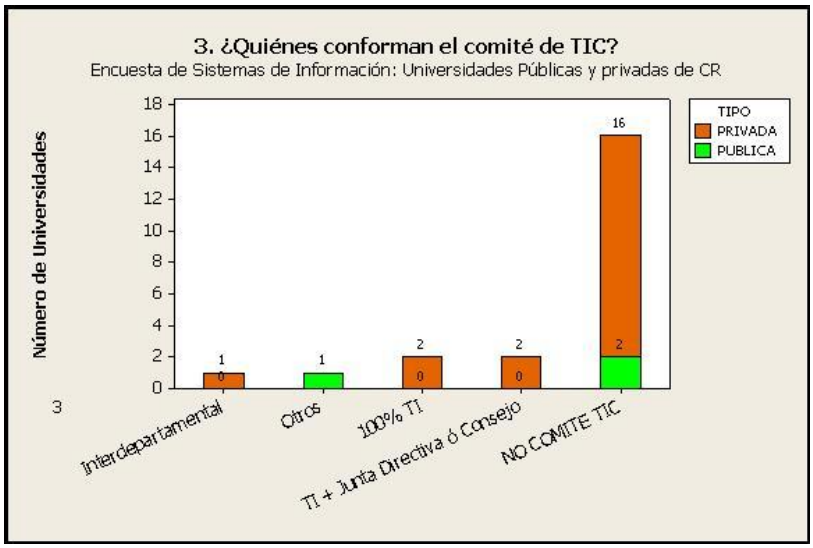


Ilustración 37

Para esta pregunta 2 universidades afirmaron que los objetivos de desarrollo de inversión son definidos por los departamentos TIC en conjunto con la Junta Directiva o Consejos, 2 universidades dicen que los objetivos son definidos 100% por los departamentos de las TIC, la única Universidad pública que tienen comité TIC manifiesta otra alternativa a las brindadas y 1 considera que los objetivos son puestos por cada departamento, unidad, Vicerrectoría, etc.

6. ¿Existe una cartera de proyectos en tecnologías de información?

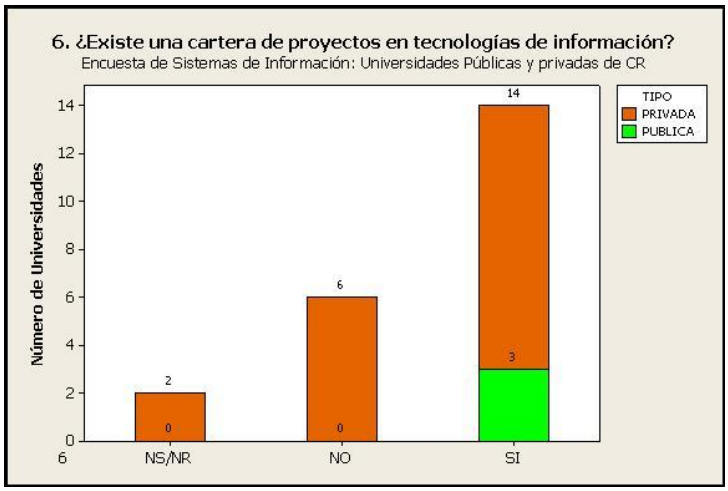


Ilustración 38

Independientemente de si tienen o no comités, se preguntó acerca de la cartera de proyectos, para la cual 2 universidades no saben o no respondieron, 6 dijeron que no y 14 dijeron que si, incluyendo a las tres universidades públicas.

7. Mencionen tres proyectos de la cartera de proyectos para el año 2007.

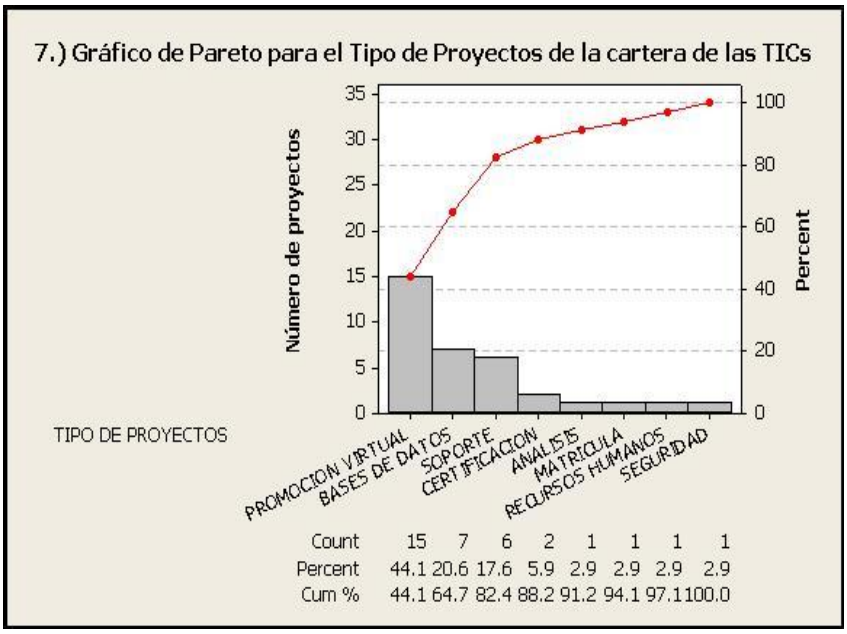


Ilustración 39

Los proyectos de las universidades que respondieron tener cartera de proyectos, se pueden clasificar en 8 grandes grupos, mediante afinidad de criterios

y luego se hizo un gráfico de pareto en el cual se muestra que el 80% de los proyectos que tienen en sus manos los departamentos TIC son referidos a Promoción virtual con 15 universidades, trabajos en Bases de datos con 7 universidades y Soporte en 6 universidades, el otro 20% se concentró en proyectos de certificación, análisis, matrícula, recursos humanos y únicamente 1 de seguridad.

8. ¿A qué plazo se desarrolla la cartera de proyectos de TI?

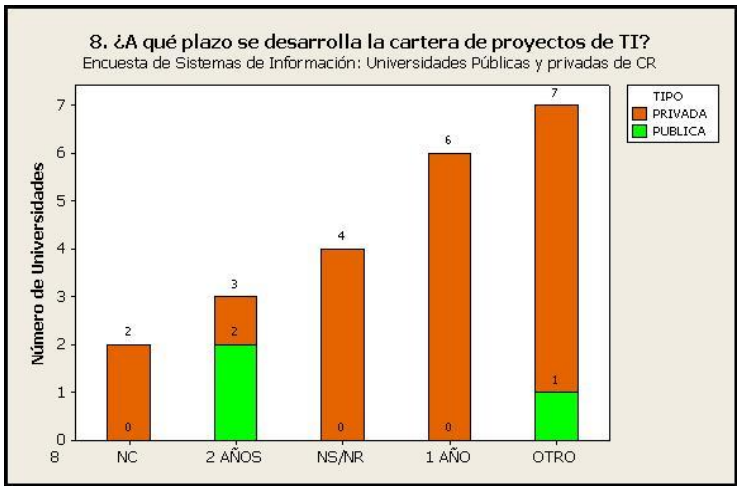


Ilustración 40

Los plazos de desarrollo de proyectos son muy variables, 3 universidades afirmaron que es de 2 años, 6 afirmaron que son de 1 año de duración, 2 no contestaron, 4 no sabían o no respondieron y 7 manifestaron otra duración diferente a las solicitadas.

9. ¿Cómo se lleva a cabo el desarrollo de proyectos?

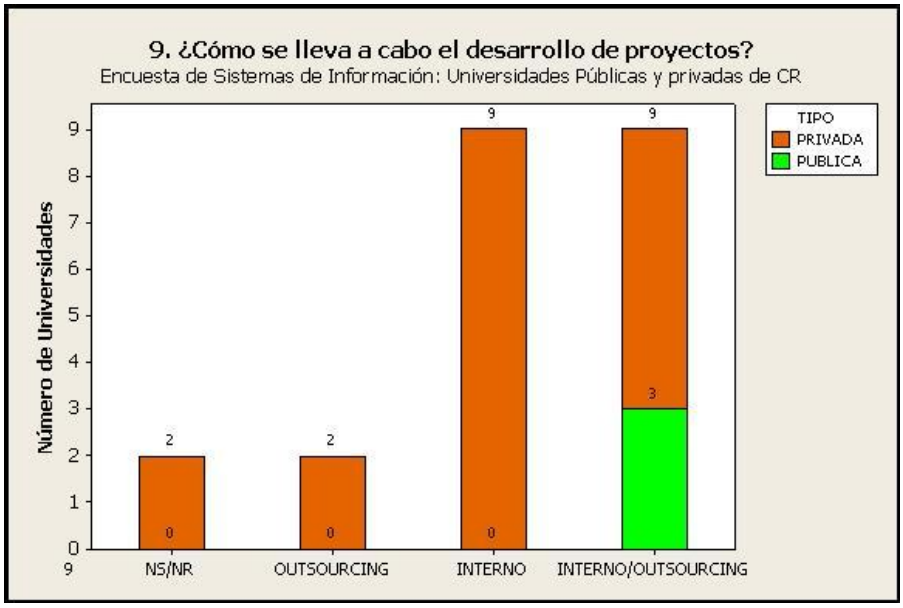


Ilustración 41

El desarrollo de proyectos se lleva a cabo en una mezcla de personal interno de las TIC y por *outsourcing* en 9 Universidades (40%), en la misma proporción de universidades se lleva a cabo solo por personal interno de las TIC, 2 universidades desarrollan sus proyectos 100% por *outsourcing* y 2 no supieron o no respondieron.

Análisis final

- **Universidades que no tienen comités de TIC**

El porcentaje tan alto de universidades que no tienen comité TIC manifiesta la desconexión que existe entre el trabajo que realizan los departamentos TIC con los objetivos que persiguen las universidades y las estrategias de las mismas para la búsqueda de competitividad.

Lo anterior se confirma, pues sería de esperar que en la pregunta de cartera de proyectos al menos el 100% conociera de que existía, sin embargo el 35% de las universidades además de no tener comités, al parecer no tienen una cartera de proyectos bien definida, lo que lleva a concluir que la principal función de los TI es de soporte.

Por otro lado, analizando el alineamiento de los departamentos TIC con la estrategia de la empresa, se puede concluir que solo el 14% de las universidades estudiadas muestran cierto alineamiento hacia la utilización de los departamentos TI con los objetivos de la universidad, tienen cartera de proyectos, realizan los desarrollos en una mezcla de personal interno de las TIC con *outsourcing*, el tiempo de los desarrollos está bien definido de 1 a 2 años, sin embargo ante la pregunta de quién define los objetivos, existe una desconexión pues en cada una se excluye la opción de que los objetivos son puestos en unión los departamentos TI con la Junta Directiva o Consejo.

- **Universidades que tienen comités de TIC**

Como se pudo apreciar con los datos, el que se tenga o no comité de las TIC es independiente de si la universidad es pública o privada.

Asimismo se concluye que existe una desconexión más con respecto a la conformación de los comités, pues únicamente en un 9% del grupo en estudio existe comunicación entre los departamentos TI con la Junta Directiva o Consejo o aún otros departamentos, a pesar de que todas respondieran que los objetivos de los TI están 100% alineados con las estrategias de las Juntas Directivas o Consejos. Por ende los objetivos de desarrollo están definidos en forma análoga al alineamiento de objetivos.

Una conclusión más acerca de encontrar una universidad bien alineada y sin desconexiones, lleva a establecer que un 14% de las universidades del país son las que presentan además de comités de TIC un buen alineamiento con la estrategia, debido a que sus desarrollos tienen plazos bien definidos, presentan cartera de proyectos y los objetivos están alineados.

Por otro lado, solo en un 5% de la población en estudio el comité de las TIC se conforma por la unión de TI más Juntas Directivas o Consejos.

Se comprueba que existe desconexión entre los objetivos, desarrollos y proyectos de los departamentos de las TI con las estrategias y objetivos Juntas Directivas y Consejos de las Universidades, independientemente de si la universidad es pública o privada.

Aun existiendo comités de TI no necesariamente existe alineamiento, pues en algunas universidades se dan dos desconexiones, una que no lo conforman la unión de varios departamentos más el personal de las TI, en algunos casos solo de las TI y la segunda que los objetivos en algunas universidades aun con comités de TI, son puestos por personal 100% de las TI, lo cual confirma la falta de alineamiento con las estrategias de las Universidades.

Desconexión relativa

Con el propósito de determinar cuán desconectada puede estar una organización, se procedió a realizar un pequeño estudio utilizando un conjunto de indicadores y dándoles un peso.

Se plantearon varios objetivos.

1. Determinar el grado de desconexión de TI con la Administración en 4 empresas, según los indicadores considerados.

2. Conocer la percepción del impacto de la capacitación de los usuarios en los sistemas de información a través del instrumento aplicado.

3. Determinar el nivel de cultura organizacional en relación con el impacto de la desconexión dentro de las empresas.

4. Identificar la influencia que tiene la Planeación Estratégica Informática (PEI) dentro del Plan Estratégico de la Empresa (PEE).

Se trabajó con una pequeña muestra conformada por cuatro empresas de los siguientes sectores: financiero, público, construcción y venta a detalle. Estas empresas son: Banco Costarricense, Ministerio Costarricense, Constructora y Súpermercado Costa Rica.

Se definieron nueve indicadores, adicionales a los veintiocho originales de la investigación base y se realizó una ponderación de cada uno de estos indicadores aplicados en el instrumento.

El instrumento fue aplicado a funcionarios y/o ejecutivos de las empresas que están en relación directa con las áreas o Departamentos de Tecnología de la

Información. Participaron un total de 29 personas de las cuatro empresas mencionadas.

En cuanto a las limitaciones se puede señalar:

- El estudio estuvo centrado en el análisis de Indicadores de Desconexión definidos en la Investigación Especial “Medición del Grado de Desconexión entre TI y la Administración de las Empresas”.
- Este análisis fue realizado con base en la caracterización de los siguientes aspectos: Cultura Organizacional, Planeación Estratégica, Capacitación y Comunicación y Uso y Aplicación de los sistemas de información.

La tecnología de información debe estar alineada con los planes estratégicos de la empresa, para lograr esto, el gerente de TI debe de participar de lleno en la elaboración del plan estratégico de la empresa y del plan estratégico de TI, para que estos sean congruentes y no haya desconexión entre TI y la administración.

El impacto del uso de los sistemas de información para la toma de decisiones es de gran importancia para una empresa. Las decisiones, con base en elementos informativos de primer orden, relevantes para el negocio tales como: estadísticas, clima, economía, inflación y otros, se tomarán con mayor seguridad, incrementando la posibilidad de ahorrar recursos.

Contar con el presupuesto adecuado para cumplir los objetivos planteados en el Plan Estratégico Informático dependerá en gran parte de la justificación que se brinde a la Gerencia, indicando el alcance y logros en el corto, mediano y largo plazo, todos enfocados a favorecer el negocio.

Los sistemas de apoyo a la toma de decisiones deben ser interactivos, ya que deben ser amigables y dar respuestas en el tiempo real para tomar decisiones importantes del negocio; tiene que ser flexible para que se acople a los distintos

sistemas que hay en la empresa y puedan interactuar entre ellos. Los sistemas deben ser de comunicación fácil, para interactuar entre la alta gerencia, los mandos medios y los operarios y viceversa; estos deben tener capacidad de desarrollar directamente modelos de dedición sin la participación operativa y profesional de los informáticos; por estas y otras razones los sistemas informáticos deben existir en una empresa, para lograr los objetivos propuestos tanto institucionales como los de TI.

Las organizaciones tienen que enfrentar algunos problemas con el personal como es la resistencia al cambio de tecnología, con máquinas más sofisticadas y aspectos de logística que deben cambiar para lograr la puesta en marcha de un nuevo sistema.

Cultura Organizacional

La cultura de una organización es un contribuyente importante o un obstáculo en la ejecución exitosa de la estrategia.

Las culturas fuertes promueven la buena ejecución de la estrategia cuando hay coincidencias y estropean la ejecución cuando hay pocas coincidencias. Una cultura profundamente arraigada y bien adaptada a la estrategia es una herramienta poderosa para la ejecución exitosa de la estrategia. Una cultura fuerte es una valiosa ventaja cuando coincide con la estrategia y una carga temible cuando no coincide.

Las culturas organizacionales cuando son adaptables son una valiosa ventaja competitiva, y en ocasiones una necesidad, en ambientes que cambian con rapidez.

Planeación Estratégica

El término Administración Estratégica se refiere al proceso administrativo de crear una visión estratégica, establecer los objetivos y formular una estrategia, así como implantar y ejecutar la estrategia, y después, con el transcurso del tiempo, iniciar cualquier ajuste correctivo en la visión, los objetivos, la estrategia, o su ejecución que parezcan adecuados.

Una visión estratégica es un mapa del futuro de la empresa que proporciona detalles específicos de su tecnología y su enfoque al cliente, la geografía y los mercados de producto que perseguirá, las capacidades que planea desarrollar y el tipo de compañía que la administración está tratando de crear. La declaración de la misión de una empresa suele centrarse en su perspectiva actual de los negocios (quienes somos y qué hacemos); describe de manera general sus capacidades, su enfoque del cliente, sus actividades y el aspecto actual de sus negocios. El modelo del negocio de una institución tiene que ver con que los aspectos económicos de su estrategia en relación con: ingresos, costos, beneficio demuestren la viabilidad de la compañía en conjunto.

Los objetivos son las metas de desempeño de una empresa, los resultados y logros que desea alcanzar. Funcionan como parámetros para la evaluación del progreso y el desempeño de la organización.

Los objetivos estratégicos se refieren a los resultados que fortalecen la posición general en los negocios y la vitalidad competitiva de una empresa; los objetivos financieros tienen que ver con las metas de desempeño financiero que la administración ha establecido que la organización debe cumplir.

La estrategia de una empresa consiste en los esfuerzos competitivos y los enfoques de negocio que los administradores utilizan para satisfacer a los clientes, competir exitosamente y alcanzar los objetivos de la organización.

La creación de una estrategia es fundamentalmente una actividad de espíritu emprendedor, impulsada por el mercado y por el cliente; las cualidades esenciales son: un talento para capitalizar las oportunidades de mercado emergentes y las necesidades en evolución de los clientes; una inclinación hacia la innovación y la creatividad; un deseo de tomar riesgos de manera prudente, y un fuerte sentido de lo que se necesita hacer para acrecentar y fortalecer los negocios.

Un plan estratégico consta de la misión y la futura dirección de una compañía, de objetivos de desempeño de corto y largo alcance, así como de una estrategia.

Capacitación y Comunicación

Enseñar las habilidades en el trabajo, recompensar el desempeño, tanto individual como de equipo, crear oportunidades de hacer carrera, tener horarios de trabajo flexibles para los empleados que son estudiantes. Contar con grupos de empleados con hábitos de trabajo positivos y actitudes corteses, capacitarlos para que actúen en formas que impresionen a los clientes y promover rápidamente a los empleados prometedores.

Proporcionales una capacitación apropiada sobre la satisfacción de los clientes y el manejo del negocio (como administradores y auxiliares por ejemplo).

La comunicación de las estrategias debe transmitir un sentido más grande del propósito, de tal manera que los trabajadores piensen que el establecimiento de la dirección a largo plazo es real. La mayoría de los miembros de la organización aceptaran el reto de ir en pos de un propósito organizacional valioso y tratarán de ser el mejor en algo que sea competitivamente significativo y valioso para los clientes.

Una visión estratégica bien articulada crea entusiasmo respecto al curso que ha trazado la administración y compromete a los miembros de la organización. Las comunicaciones en una organización que están mejor redactadas, arrojan luz de un modo claro y emotivo sobre la dirección hacia la que se dirige la empresa.

Un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio.

Uso y Aplicación de los Sistemas de Información

El cliente de TI en muchas ocasiones es difícil ya que este tiene una resistencia al cambio por nuevos sistemas para adaptar nuevas tecnologías a la empresa. Generalmente hacen caso omiso de las políticas de protección a favor de los sistemas de las empresas; por otro lado en ocasiones no quieren dejar sistemas viejos de control por otro más rápido para su uso y dar información más segura.

Dentro de las tecnologías de información básicas se tienen una serie de componentes a saber: la unidad central de almacenamiento, la memoria principal, dispositivos de entrada (el teclado, ratón y otros); dispositivos de salida (monitores, impresoras y otros); dispositivos de entrada y salida (tarjetas de red y módems); dispositivos de almacenamiento (discos duros, diskettes, memorias tipo *flash* y otros).

En el contexto de la investigación especial, se realizó una ponderación de los indicadores integrantes del instrumento, en las siguientes categorías: Importante (peso 1), Muy importante (peso 2) y Crítico (peso 3).

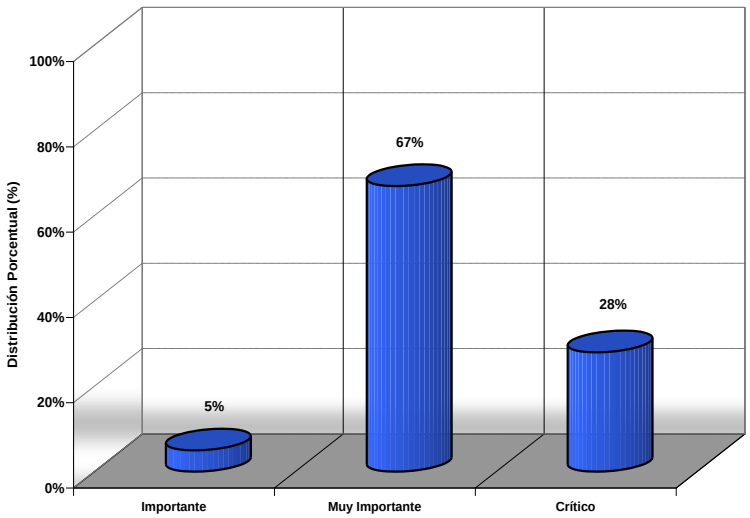


Ilustración 42

Con el fin de analizar la Ponderación de los Indicadores, se definieron cuatro categorías dentro de las cuales se pueden agrupar los indicadores.

Obtener un bajo grado de desconexión dependerá del éxito (percepción reflejada en resultados dentro de las empresas) que dentro del contexto de cada empresa alcancen cada una de las siguientes categorías:

- Cultura Organizacional
- Planeación Estratégica
- Capacitación y Comunicación
- Uso y aplicación de los SI

La suma de las iniciativas en que incurra la empresa en relación con las categorías mencionadas, con el objetivo de minimizar la desconexión, va a determinar el grado de desconexión que tenga cada empresa (éxito= grado de desconexión bajo, fracaso= grado de desconexión alto).

Con base en las cuatro categorías mencionadas, las cuales conforman parte de las variables que se consideraron para la ponderación final, se les dio un

“peso” en referencia al nivel de su impacto dentro de la organización y la desconexión:

- Cultura Organizacional 30%
- Planeación Estratégica 35%
- Capacitación y Comunicación 20%
- Uso y aplicación de los SI 15%

Dentro del instrumento utilizado, la cultura organizacional tiene que ver con:

- Prioridad que tiene TI en los mandos altos de la organización.
- Políticas institucionales de TI.
- Manejo del presupuesto de TI dentro de la empresa.
- Ubicación de TI dentro del organigrama de la empresa.

El gráfico siguiente muestra los resultados de esta categoría en las cuatro empresas estudiadas:

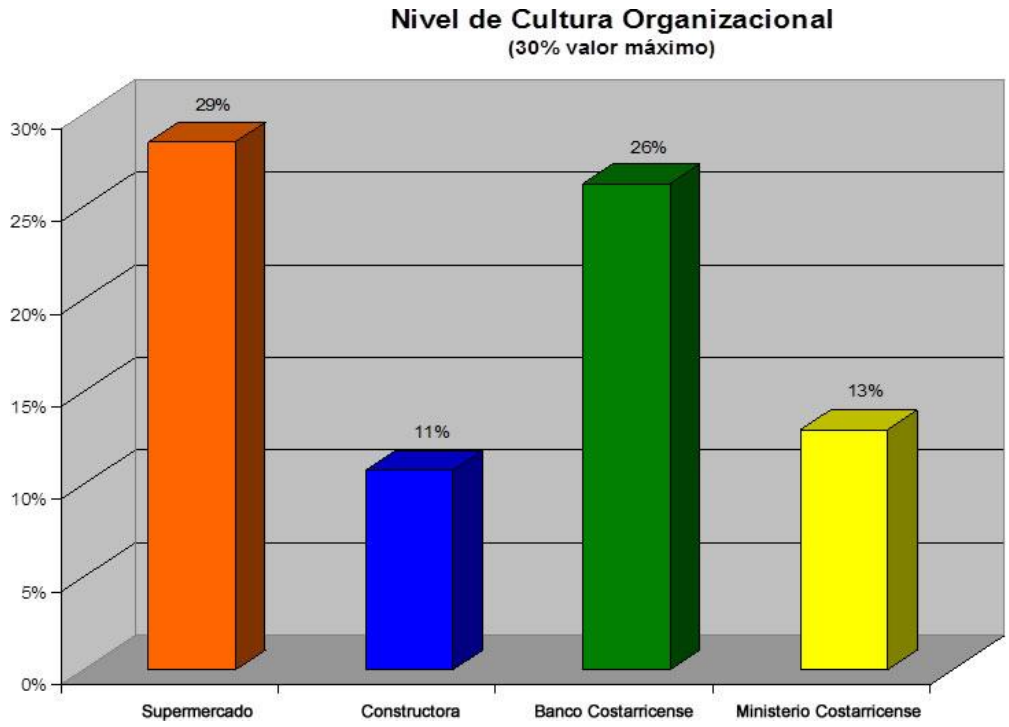


Ilustración 43

Planeación Estratégica

Los indicadores buscan información de:

- Existencia de un Plan Estratégico en la empresa (PEE).
- Existencia de un Plan Estratégico Informático en la empresa (PEI).
- Alineamiento entre el PEE y el PEI en la empresa.
- Participación de TI en la organización.

El gráfico siguiente muestra los resultados de esta categoría en las cuatro empresas estudiadas:

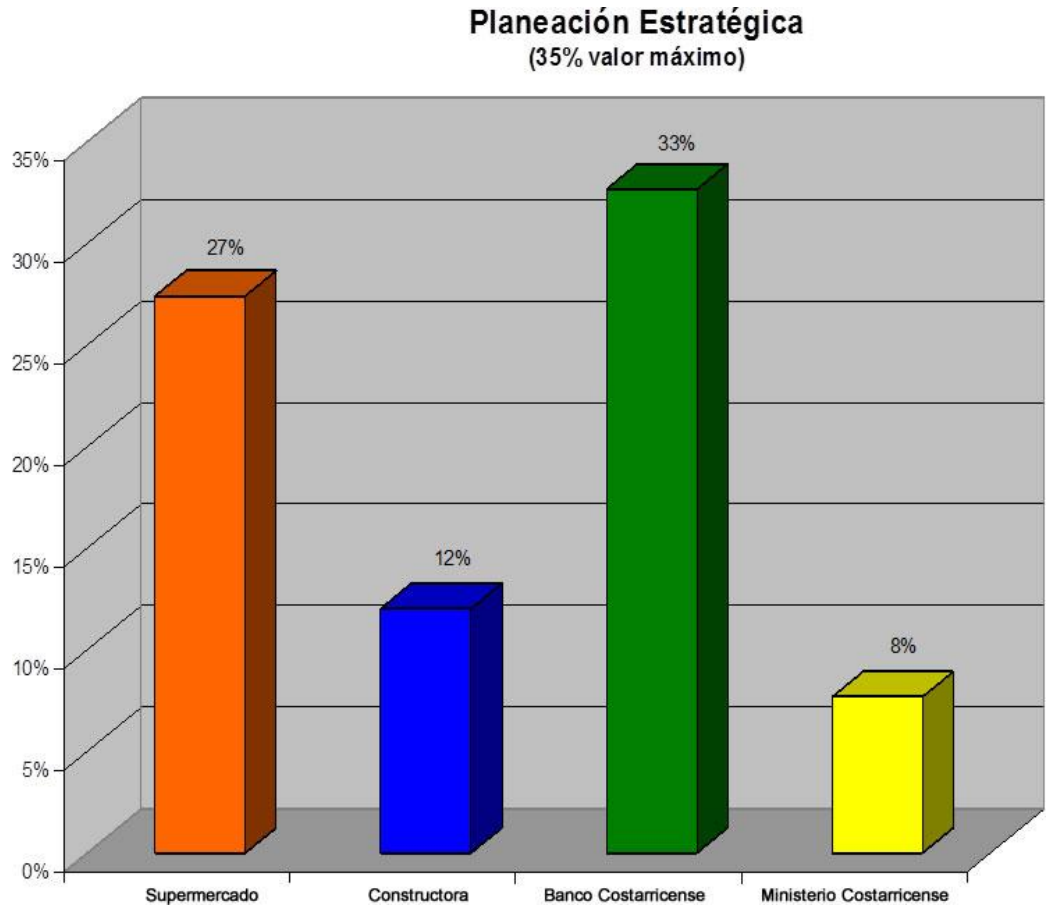


Ilustración 44

Capacitación y Comunicación

Los indicadores relacionados con la capacitación y la comunicación interna de las empresas, se relacionan con:

- Capacitación en el uso adecuado de la tecnología.
- Comunicación interna en la organización.
- Conocimiento de las políticas institucionales de TI por parte de los clientes.

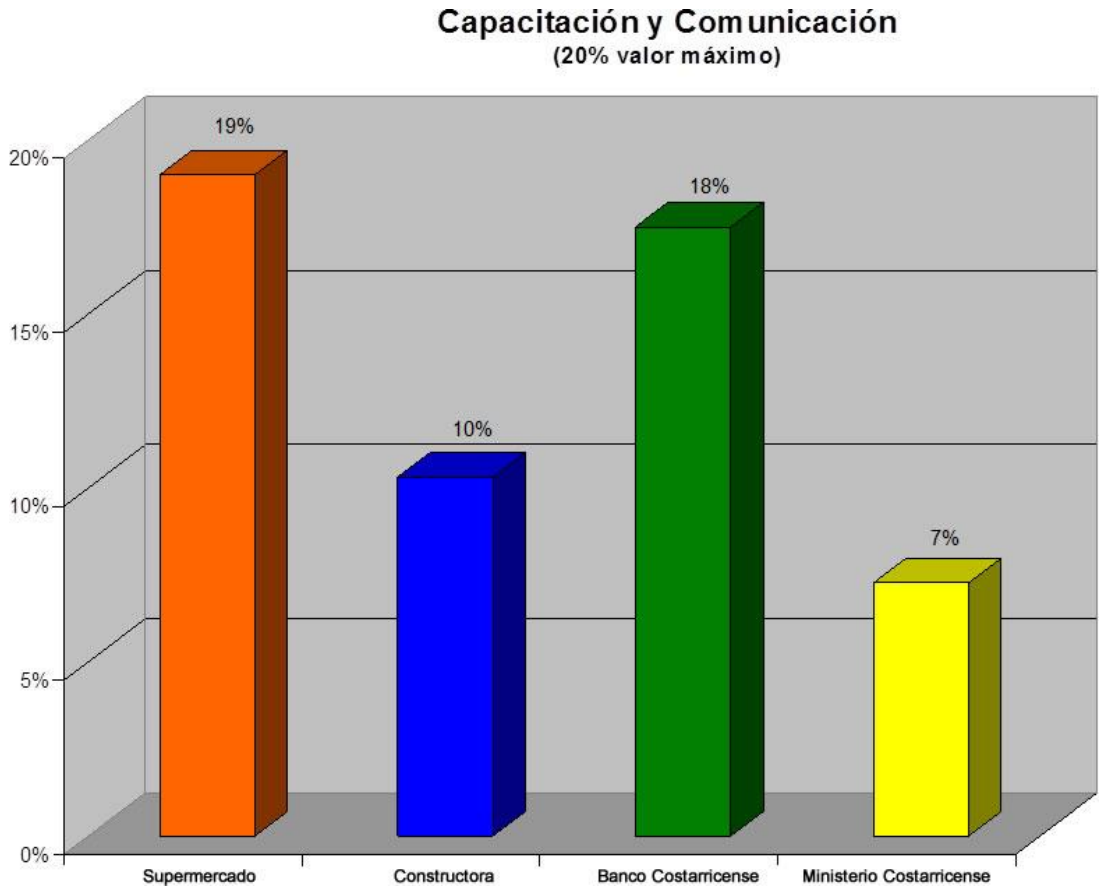


Ilustración 45

Uso y aplicación de los sistemas de información

Conocer y saber utilizar los sistemas de información con que cuenta cada compañía, se investigaron por medio de los indicadores preguntando acerca de:

- Participación del usuario dentro de los proyectos de TI.
- Uso de los SI por parte del cliente.
- Grado de libertad del cliente en el uso de los SI.
- Cultura informática en la organización.
- Manejo de información confidencial por parte de los clientes.

El gráfico siguiente muestra los resultados de esta categoría en las cuatro empresas estudiadas:

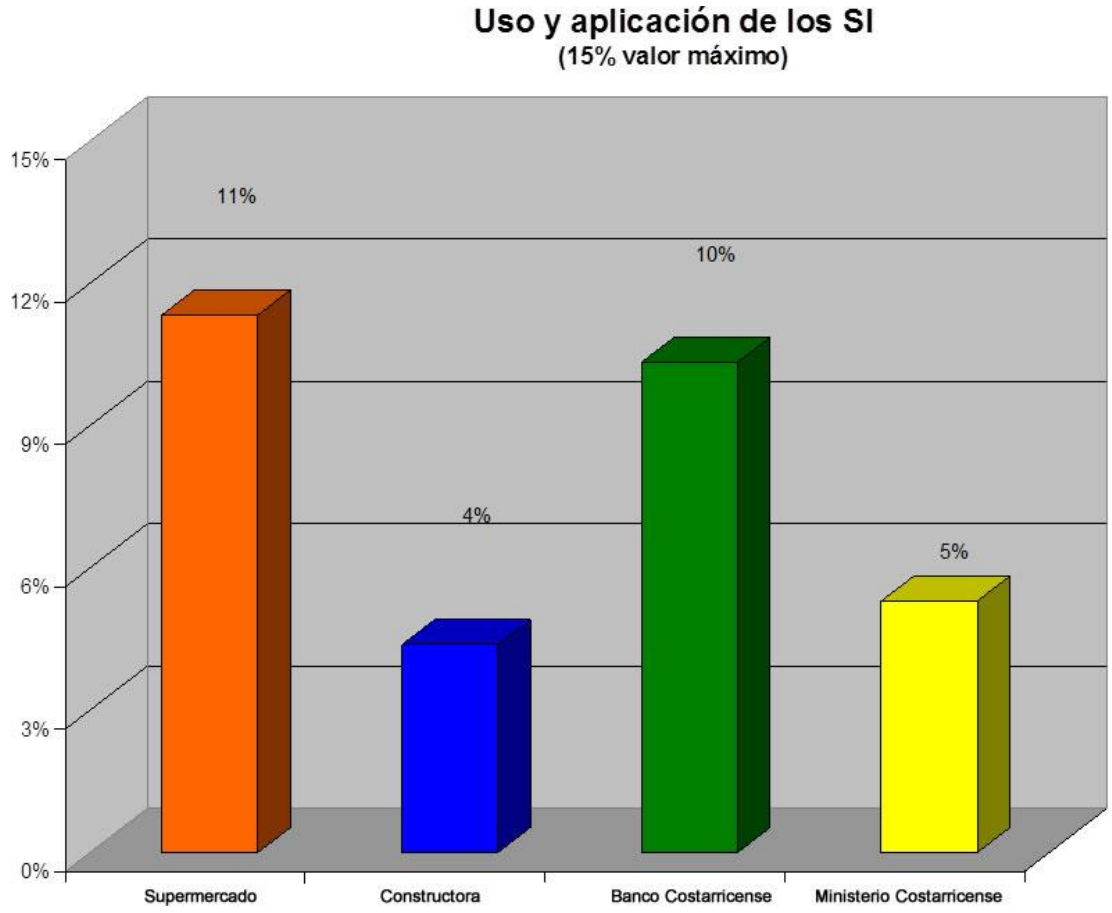


Ilustración 46

Indicadores más representativos

Una vez definidas las categorías analizadas por medio del instrumento de indicadores, y los pesos que las mismas tienen para el análisis, se consideró necesario presentar los resultados de los indicadores más representativos.

Cultura Organizacional

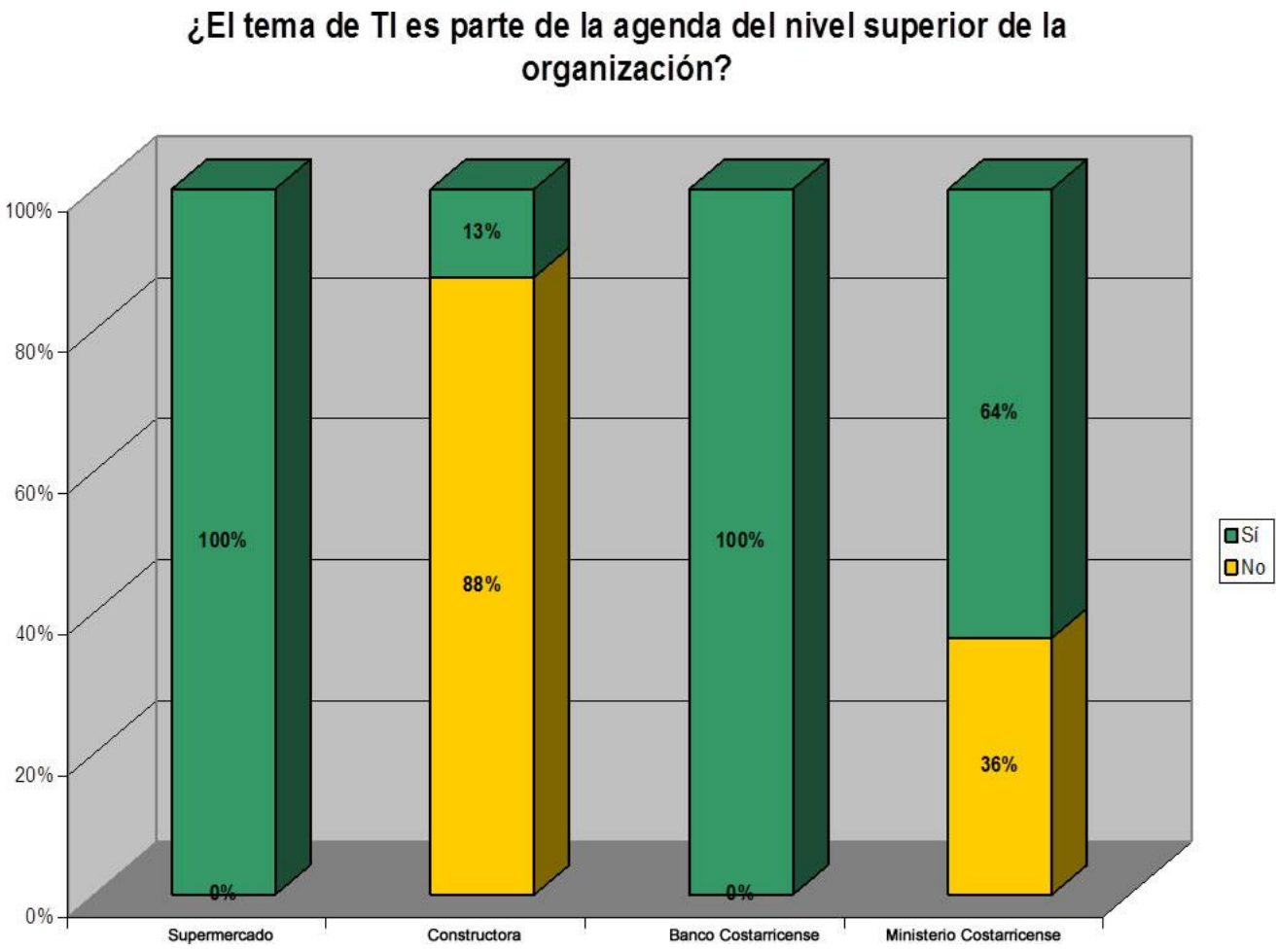


Ilustración 47

Planeación Estratégica

¿Está alineado el PEI con el PEE?

Un 80% de los entrevistados en Súpermercado, 25% en Constructora, 100% en el Banco Costarricense y 82% en el Ministerio Costarricense, indicaron que sí estaban alineados.

Capacitación y Comunicación

¿Cuentan los usuarios con la capacitación suficiente para la utilización de las tecnologías de información de la organización?

El 80% de los entrevistados en Súpermercado, 75% en Constructora, 60% del Banco Costarricense y 9% en el Ministerio Costarricense indicaron que sí. Sin embargo a pesar de las buenas calificaciones en Súpermercado y el Banco Costarricense, los números arrojan información interesante. Se percibe falta de capacitación.

Uso y aplicación de los sistemas de información

¿Puede usted descargar software libremente en Internet?

Un 88% de los entrevistados en Constructora, 80% del Banco Costarricense y 36% del Ministerio Costarricense manifestaron que sí pueden hacerlo. Si no hay políticas adecuadas para efectuar descargas de software de lugares o sitios seguros, la información puede quedar comprometida en cualquier momento, se pueden recibir ataques que produzcan daños serios en la información y los sistemas de estas organizaciones. El 100% de los entrevistados en Súpermercado indicaron que no pueden hacerlo libremente.

Uso y aplicación de los sistemas de información

¿Cada cuánto realiza usted el cambio de su clave dentro del sistema?

Las respuestas acumuladas dejan mucho que desear pues indica que no hay políticas claras en este sentido y es consecuente con problemas de capacitación.

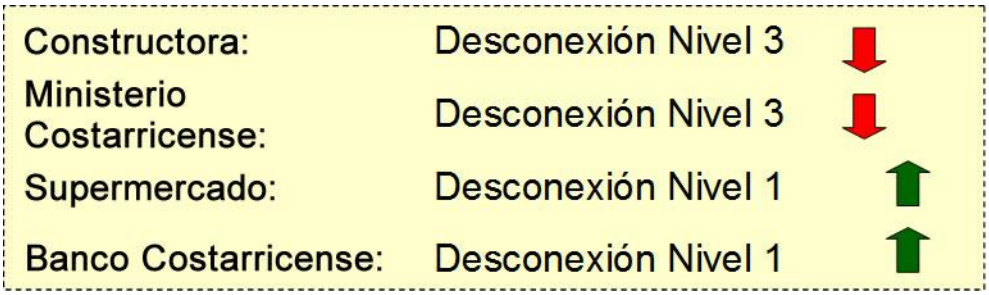
Un 48% de todos los entrevistados manifestaron que cambian su contraseña tan solo una vez al año, un 34% nunca lo hacen y tan solo un 18% de uno a tres meses. Las contraseñas son el primer eslabón en la protección de la información desde el punto de vista de acceso por los usuarios. Si a esto se suma que muchas personas utilizan claves débiles o bien las dejan en lugares accesibles por terceros, es definitivo entonces que se hace más que necesario el implementar políticas adecuadas en este sentido.

Niveles de Desconexión

Con base en los resultados de la aplicación de los Indicadores a la muestra, para el caso de las cuatro empresas en cuestión, se definen niveles de desconexión dependiendo de la criticidad.

Desconexión Nivel 1: Nota mayor o igual a 76%
Desconexión Nivel 2: Nota entre 51% y 75%
Desconexión Nivel 3 Nota entre 26% y 50%
Desconexión Nivel 4: Nota entre 0% y 25%

Mediante la combinación algorítmica de las variables (categorización, peso de los indicadores e impacto de las categorías en la organización) se define que los siguientes son los niveles de Desconexión para cada una de las empresas estudiadas:



Lo anterior es de gran utilidad con los indicadores que se plantearon y tratando de no concentrase en el alineamiento por sí mismo, puesto como ya se ha explicado, la desconexión toma en cuenta más variables que el sólo alineamiento.

Teoría de las etapas de Nolan

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 no 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.

Etapa 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 5

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%

Tabla 5

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 interfaces 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 interfaces 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 interfaces 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 logar 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 viaja data.

Charles B. Wang se atreve a asegurar que las organizaciones que eliminen o disminuyan 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."[13]

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.

[13] (Wang:40)

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 pude 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* (Cassydy, 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 los 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 Leveque***, 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 logar 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 poissoning,* 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 que la información sea comprometida

Las estrategias en este caso deben obedecer a principios fundamentales puesto que ellas 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."[14]

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."[15]

[14] (Nicholls:28)
[15] (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 hirviente; 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.

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 cuido, 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). 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. Esta empresa en 2004 inició la transformación de un ISP a un ASP. En la actualidad 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.

V. CONCLUSIONES Y RECOMENDACIONES

Ha quedado claro que sí existe una relación estrecha entre el fenómeno de la desconexión tal como se ha explicado y problemas de seguridad. Si no existe una cultura de aseguramiento de la información, la probabilidad de que una amenaza se concrete debido a una vulnerabilidad es relativamente alta. ¿De qué

depende que una organización reciba un ataque? Depende de muchos factores y de su grado de exposición, de los intereses de los actores involucrados ya sea por la información misma o, como se explicó en el Capítulo I, de sus motivaciones.

Los aspectos más importantes que deben ser abordados por las organizaciones para desarrollar una cultura integral de aseguramiento de la información, pueden ser agrupados en cinco grandes aspectos, administración de la seguridad, aplicaciones de misión crítica, parque de computadores instalados, redes y administración de sistemas.

Cada uno de los aspectos anteriores engloba una serie de principios y prácticas que deben ser cubiertos por cualquier organización que desee minimizar ataques a su información.

Esta tesis no pretende convertirse en un manual de mejores prácticas pero se hará un esbozo para mitigar los posibles ataques, considerando las estrategias presentadas en el capítulo anterior más algunos lineamientos generales. Se recomienda visitar el sitio www.sans.org donde se halla en forma pormenorizada una descripción de políticas que cubren todos los aspectos importantes que deben ser tomados en el establecimiento de la política de seguridad de una organización.

En este capítulo se esboza un aspecto fundamental para generar una cultura de aseguramiento de la seguridad. Este se subdividió en áreas y las áreas en secciones, con el propósito de minimizar que la información sea comprometida y en especial para dar respuestas a las debilidades encontradas en cada una de las investigaciones objetos de esta tesis.

Es importante dejar claro que un cambio cultural toma tiempo y en este sentido, el papel que debe desempeñar la Alta Dirección es fundamental; ellos se deben constituir en los abanderados de una causa que aunque difícil, debe

enfrentarse, pues no se pone en tela de discusión que la información es uno de los activos más importantes en las organizaciones.

Aspecto: Administración de la seguridad

Para mantener bajo control los riesgos a que puede estar sujeta la información y dañar a una entidad se requiere de una clara directriz de la Alta Dirección y un fuerte compromiso de ella, una adecuada asignación de recursos, una capacitación constante que posicione buenas prácticas de aseguramiento de la información a través de toda la organización y que se pueda establecer un ambiente seguro.

Área: Dirección de alto nivel

Para alcanzar un alto nivel, consistente y eficaz de buenas prácticas de seguridad para el aseguramiento de la información, es necesaria una clara dirección de la Alta Administración. Esta especifica las políticas de seguridad de la información y genera los compromisos que deben ser aceptados por los colaboradores directos que tienen acceso a cualquier tipo de información dentro de la entidad.

- Sección: Compromiso de la administración
- Objetivo: Establecer el compromiso de la Alta Dirección con el aseguramiento de la información.
- Sección: Política de seguridad
- Objetivo: Desarrollar, implementar y comunicar una política de seguridad de la información para todos los individuos que puedan acceder a la información y a los sistemas de la entidad
- Sección: Acuerdos para el personal

- Objetivo: Establecer acuerdos de confidencialidad con el personal de la entidad, donde también se especifiquen las responsabilidades por la información que utilice, acceda, modifique, elimine, etc.

Área: Organización de la seguridad

El resguardar adecuadamente los sistemas de información, la información misma, etc. requiere que todas las actividades encaminadas a su protección, sean organizadas apropiada y eficazmente. Además, todo el personal de la organización debe desarrollar las habilidades necesarias para utilizar de manera correcta los sistemas de información.

- Sección: Control de alto nivel

- Objetivo: Debe proveerse una estructura del tipo arriba hacia abajo mediante un equipo de trabajo de alto nivel (comité de informática o similar) que verifique que se lleve a cabo todas las actividades de seguridad que se haya implementado; este comité debe depender de la Alta Administración.

- Sección: Función de la seguridad de la información

- Objetivo: Establecer la posición de especialista de seguridad de la información, con la responsabilidad de promover las políticas de seguridad en toda la organización y coordinar todas las actividades relacionadas.

- Sección: Educación sobre seguridad

- Objetivo: Proveer la capacitación y educación necesarias para que el personal desarrolle las habilidades requeridas para ejecutar los sistemas de manera apropiada, y, en especial, para que cumplan con las responsabilidades en cuanto al resguardo y manejo apropiado de la información.

Área: Requerimientos de seguridad

Hay que garantizar que las medidas aplicadas de acuerdo a la política para salvaguardar la información son proporcionales a su importancia para el negocio, según las mejores prácticas, y que la información se ha clasificado de manera apropiada asignando su pertenencia (*ownership*) y la identificación correcta de los riesgos.

- Sección: Clasificación de la seguridad
- Objetivo: Establecer un esquema de clasificación de la seguridad de la información, basado según su sensibilidad.
- Sección: Propiedad (*ownership*) de la información
- Objetivo: Lograr que el personal de la entidad obtenga un sentimiento de propiedad (*ownership*) de la información y pueda responder a esa mayordomía adquirida por él con base en su compromiso.
- Sección: Análisis del riesgo de la información
- Objetivo: Habilitar a los individuos que son responsables del manejo de la información y de los sistemas asociados, para que identifiquen los riesgos a que está sometida la información bajo su cuidado, y que sean capaces de desarrollar e implementar los controles apropiados para mantener esos riesgos dentro de límites aceptables.

Área: Ambiente seguro

No es una tarea fácil el desarrollar una cultura de aseguramiento de la información. Para coadyuvar en ese logro, es necesario que se desarrolle el marco apropiado y la disciplina que permitan que las mejores prácticas se constituyan en un pilar de toda la organización. No debe permitirse que por tener un oficial de

seguridad, llegue a creer que es responsabilidad de ese individuo el logar este tipo de cultura y menos que él es el responsable de la información de la entidad.

- Sección: Privacidad de la información
- Objetivo: Deben establecerse controles que garanticen la privacidad de la información personal que impidan que ésta pueda ser utilizada de manera no apropiada y garantizar que se cumple con las disposiciones que en materia legal se hayan dictado sobre ella.
- Sección: Administración de los activos
- Objetivo: Debe llevarse un inventario adecuado sobre los activos *hardware-software* además utilizar equipos
- Sección: Protección física
- Objetivo: Restringir el acceso físico a los lugares y a los a los equipos donde se almacenan los sistemas y la información de la organización a personas no autorizadas, para evitar accidentes o ataques sobre ellos.
- Sección: Continuidad de negocios
- Objetivo: Establecer procedimientos estándar y planes para mantener la continuidad de operación de los sistemas de la organización

Área: Ataques maliciosos

Las organizaciones están expuestas a ataques por parte de terceros, pueden ser virus, "*hacking*", *malware* de todo tipo o ataques físicos.

- Sección: Protección contra virus, troyanos, código malicioso, etc.
- Objetivo: Deben establecerse políticas adecuadas para defenderse del ataque de virus, troyanos, código malicioso (*rootkits*), y

desarrollarse procedimientos adecuados para aplicar vacunas ante una infección.

- Sección: Detección de intrusos
- Objetivo: Deben establecerse mecanismos de detección de intrusos y de respuesta si se han causado daños.
- Sección: Respuesta ante emergencias
- Objetivo: Procedimientos para responder ante emergencias así como equipos para atenderla, deben ser establecidos en el evento de un ataque, con el propósito de reducir el impacto sobre el negocio.
- Sección: Administración de las actualizaciones (parches)
- Objetivo: Debe establecerse una estrategia adecuada para garantizar que las actualizaciones sobre los sistemas se haga tan pronto estén listas las actualizaciones (parches) a los sistemas de base.

Área: Miscelánea

En esta área se cubren una serie de tópicos que emergen con rapidez en una disciplina cambiante como lo es el aseguramiento de la información. Tales como criptografía, llaves públicas, correo electrónico, trabajo remoto, *outsourcing,* comercio electrónico y otras semejantes.

Sección: Criptografía

Objetivo: Utilizar la criptografía para proteger información sensible y garantizar que se utiliza de manera correcta

Sección: Claves o llaves públicas (PKI)

Objetivo: Garantizar que la infraestructura de llave pública está protegida y que se han fortalecido todos los elementos asociados, tanto de sistemas operativos como de resguardo de la clave y de acceso a la Autoridad Certificadora

Sección: Correo electrónico

Objetivo: Proteger el sistema administrador del correo electrónico mediante una adecuada combinación de políticas de seguridad, procedimientos y controles técnicos, que garanticen la disponibilidad del servicio, la confidencialidad y la integridad de los mensajes y sus adjuntos.

Sección: Trabajo remoto

Objetivo: Garantizar que los equipos de los colaboradores que acceden en forma remota los servidores centrales y las redes empresariales, lo hacen de la manera que dicta la política y que no comprometen la información.

Sección: Acceso por terceros

Objetivo: Asegurar que el acceso por terceros sea de acuerdo a los privilegios que se le han asignado y que se identifican adecuadamente.

Sección: Comercio electrónico

Objetivo: Establecer el marco apropiado y las medidas de seguridad pertinentes que garanticen que las transacciones electrónicas son seguras.

Sección: Mensajes instantáneos

Objetivo: La mensajería instantánea es uno de los factores de riesgo más graves en una organización, por lo tanto deben diseñarse procedimientos y normas que garanticen la confidencialidad e integridad de los mensajes en tránsito y reducir la probabilidad de ataques por su medio a través de la implementación de contramedidas adecuadas.

Lo anterior es solo una muestra de lo que se debe hacer. Para lograr una adecuada defensa de la información, no debe dejarse por fuera ningún otro aspecto. Deben diseñarse políticas dirigidas a las aplicaciones de misión crítica, instalación de redes y computadores, sistemas operativos, redes de voz, desarrollo de sistemas, que garanticen los controles adecuadas sobre cada uno de esos aspectos. No pueden dejarse por fuera cosas que se consideran tan sencillas como efectuar respaldos con la periodicidad que se determine, auditorías de las normas y procedimientos y de las mismas políticas, configuración de los equipos móviles, de los computadores personales y de los de escritorio, conexiones, diseño de páginas web transaccionales, protección contra incendio, inundaciones o cualquier otro desastre natural, fuentes de energía, procesos de autenticación, etc.

Lo anterior se puede lograr desarrollando un plan estratégico de seguridad de la información, que será parte del PEI, mediante el cual la organización compromete recursos suficientes para salvaguardar ese activo tan valioso, la información.

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 desparezca.

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 Comunications 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.hping.org

http://www.symantec.com

http://www.foundstone.com

http://www.purge-it.com

http://www.stegoarchive.com/

APENDICE I

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

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?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
18	¿Se utilizan los sistemas en producción para apoyar la toma de decisiones?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
19	¿Cuentan los usuarios con la capacitación suficiente para la utilización de las tecnologías de información de la organización?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
20	¿Cuenta la organización con políticas institucionales en TI aprobadas?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
21	¿Cuál es el nivel de auditoría de sistemas en la organización?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
22	¿Existe un nivel elevado de cultura informática en la organización?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
23	¿Conoce los procedimientos para gestionar necesidades o	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

	requerimientos ante TI?						
24	¿Es entendible el lenguaje con que se comunica TI?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
25	¿La opinión de TI es considerada en la toma de decisiones que le afectan?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
26	¿Es fácil obtener soluciones con TI?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
27	¿Comunica TI información importante a sus clientes (planes, cambios)?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
28	¿TI analiza riesgos y oportunidades que afectan el desarrollo de los negocios?	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

APÉNDICE II

Instrumento utilizado

#	INDICADOR
1	¿Existe un plan estratégico en la empresa?
2	¿Depende el gerente de Tecnologías de Información (**TI**) del nivel superior de la organización?
3	¿Existe un grupo de alto nivel que priorice el desarrollo de la tecnología?
4	¿Se cuenta con un Plan Estratégico de TI?
5	¿Se elabora el Plan Estratégico de Informática (**PEI**) de manera conjunta entre los niveles gerenciales de la empresa y TI?
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 (en uso o en desarrollo) satisfacen las necesidades de información de los usuarios?
17	¿Los sistemas de información se adaptan fácilmente a las necesidades del negocio?
18	¿Se utilizan los sistemas en producción para apoyar la toma de decisiones?
19	¿Cuentan los usuarios con la capacitación suficiente para la utilización de las tecnologías de información de la organización?
20	¿Cuenta la organización con políticas institucionales en TI aprobadas?
21	¿Cuál es el nivel de auditoría de sistemas en la organización?
22	¿Existe un nivel elevado de cultura informática en la organización?
23	¿Conoce los procedimientos para gestionar necesidades o requerimientos ante TI?
24	¿Es entendible el lenguaje con que se comunica TI?
25	¿La opinión de TI es considerada en la toma de decisiones que le afectan?
26	¿Es fácil obtener soluciones con TI?
27	¿Comunica TI información importante a sus clientes (planes, cambios)?
28	¿TI analiza riesgos y oportunidades que afectan el desarrollo de los negocios?
29	Cada cuánto realiza el cambio de la clave de ingreso al sistema?
30	Conoce usted si existen sanciones por no cambiar la clave a tiempo (esto es una política, es decir, automáticamente el sistema solicita el cambio de contraseña, de no realizarse la cuenta se bloquea)
31	Puede usted descargar software de Internet libremente?
32	Tiene usted acceso a correo electrónico diferente al de su empresa desde las computadoras de la compañía?
33	Tiene usted disponibilidad para llevarse la computadora personal o información de la empresa a su casa?
34	Ha tenido usted problemas con su trabajo porque no ha comprendido alguna indicación del área de TI?
35	Se realizan auditorías de sistemas en su lugar de trabajo, si SÍ, indique frecuencia.
36	Sabe usted si el equipo de su departamento está dentro de un inventario de control de hardware.
37	Conoce usted si existen políticas punitivas (de sanción legal) ante la fuga de información de la empresa?

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.