Conferencia Chicago II

Estimados colegas

En función de haber asistido a los Eventos citados en la referencia, reflejo a continuación una síntesis de los aspectos más relevantes acontecidos:

1) FORO GLOBAL Y TALLER DE LIDERAZGO 2005

***IIA:** Se desarrollaron los siguientes temas: Organigrama de la Casa Central Global, Equipo y Relaciones con los Capítulos (156) y Afiliadas (91) y Servicios a la membresía. Lo más destacado en este punto es:

a) El IIA es una organización global que está siendo más global cada día. Dos hitos así lo demuestran: 100.000 Socios y 50.000 CIA's (Certified Internal Auditor) al 30-06-2005.

b) La reciente designación del sr. Victor García como Gerente Regional para el área de Latinoamérica y Caribe, la cual incluye una relación directa con FLAI (Federación Latinoamericana Auditores Internos).

c) El IIA ha conformado un Plan Estratégico para el período 2005-2007,el cual define como Misión la de ser la voz global de la profesión de auditoría interna, defendiendo su valor, promoviendo las mejores prácticas y proporcionando servicios a sus socios. Las actividades en apoyo de esta Misión son, entre otras, las siguientes: 1) Resaltar el valor que los auditores internos agregan a sus organizaciones; 2) Generar oportunidades integrales de educación y desarrollo profesional, normas y otras guías para el ejercicio profesional, y programas de certificación; 3) Investigar, difundir y promover entre los profesionales y partes interesadas conocimientos respecto de la auditoría interna y su función apropiada en el control, gestión de riesgos y gobierno; 4) Educar a los profesionales y otros públicos relevantes respecto de las mejores prácticas en auditoría interna, y 5) Reunir a los auditores internos de todos los países para compartir información y experiencias.

d) La importancia de ser CIA (Certified Internal Auditor), pues esta es la única certificación para auditores internos reconocida mundialmente, cuyo examen se ofrece en más de 250 sitios en 80 países y la cual se recomienda muy especialmente su obtención para aquellos que desarrollan funciones de Directores Ejecutivos, Gerentes y Personal de Auditoría y Personal de Gestión de Riesgos.

***Debate de Temas:** a) Defensa de la Profesión; b) Aseguramiento de Calidad; c) El valor de ser socio del Instituto.

2) 64° CONFERENCIA INTERNACIONAL 2005

*A dicha Conferencia asistieron 2.400 participantes, representando a 85 países. Esta es la sexta ocasión en que la ciudad de Chicago sirve de anfitrión para la realización de este evento, y en su apertura contó con la presencia y disertación del Gobernador del Estado de Illinois-USA.

*Tuvo en total 94 sesiones educativas - sólo 14 de ellas contaron con traducción simultánea al español -, divididas en 11 Secciones según detalle: 1) Gerenciamiento de la Auditoría; 2) Fraudes 2005; 3)Sarbanes-Oxley: Presente y Futuro; 4) Desarrollo en Sistemas de Auditoría; 5) Mejores Prácticas en AI; 6) Gerenciamiento de Riesgos; 7) Crecimiento Profesional; 8) Gobierno Corporativo; 9) Temas Generales de Auditoría; 10) Auditando Servicios Financieros; 11) Aplicaciones Informáticas de AI.

***El detalle de las sesiones a las que asistí es el siguiente:**

1) El Auditor Interno: Elevando las expectativas al próximo nivel - Sharon Allen,Chairman of the Board , Deloitte; 2) El nuevo Rol de la AI en el Gobierno Corporativo - Bruce Adamec, Vice President and General Auditor, United Stationers Inc; 3) Lecciones Aprendidas de Fallos Corporativos - Cynthia Cooper, President CC Consulting; 4) Control a través del Monitoreo Continuo - John Verver, Vice President ACL; 5) Balanced Scorecard - Declan McLaughlin, Audit Manager, National Grid Transco; 6) Fijando Normas de Contabilidad y Auditoría - Larry Rittenberg (Chairman IIA); 7) Outsourcing Sistemas de Información - Reeti Nair, President Aligna, Inc / R. Moller President Compliance & Control Systems Inc/G Casal Director IFPC; 8) Aplicación Efectiva de IIA Standards - Andrew Dahle, Partner PriceWaterhouseCoopers; 9) SOX: ¿ Qué sigue ? - Ed Duddley, General Auditor ABB Americas; 10) Gobierno Corporativo. Perspectiva del CEO - Phil Livingston, Vice Chairman, Approva Corporation; 11) ¿Está Usted listo para el Éxito ? - Rebecca Ryan, President, Next Generation Consulting, Inc.

***Vale la pena exponer algunos conceptos e ideas en las que, los distintos expositores han puesto FOCO:**

a) La Función de AI

Permite recuperar la confianza del inversor. Ello es así puesto que nuestra especialización ha madurado interesantemente, lo cual deriva en poder encarar los actuales desafíos con una mayor responsabilidad dando así una adecuada respuesta a las necesidades de nuestros clientes.

b) El Rol del AI,

Se lo define como crítico pero delicado a la vez. Ha tenido un desarrollo que a la fecha tiene más trabajo y responsabilidad y que demanda de un compromiso sólido, ya que es este Rol el centinela de la responsabilidad empresarial. Honestidad, integridad y profesionalidad: indispensables para llevar adelante el día a día. Lo que no puede faltar es el VALOR para decir las cosas como son, con la debida PRUDENCIA y OPORTUNIDAD que el tema requiera (no hay que disfrazar las cosas). O en otras palabras, Diplomáticos pero Honestos y Justos.

c) ¿Sobre quiénes debemos ejercer Influencia?

Sobre aquéllas partes interesadas que puedan potenciar el conocimiento e intereses que se tengan de la profesión de AI: Consejos de Administración, Comités de Auditoría, Presidentes Ejecutivos (CEOs), Directores Financieros (CFOs), Auditores Externos y Organismos de Supervisión / Regulación.

d) Hacia adónde vamos?

Hay que poner a prueba el status quo y seguir pensando cómo hacer las cosas mejor. No olvidemos que el Gobierno Corporativo no es sino un balance de Poderes entre la Gerencia, la Dirección y el Accionista. Y tener un buen equilibrio de las partes, es responsabilidad de todos. Hay que promover la buena salud dentro de la Dirección; para ello debemos ser creíbles y eso implica estar listos y preparados. Qué esperamos recibir a cambio? Ser valorados, respetados y apreciados por la Gerencia, por la Dirección y también por el Accionista.

e) Gobierno Corporativo.

• El Directorio es el responsable del sistema de control interno y esto incluye la elección del Auditor Externo y su remuneración,

• La Gerencia debe tener su propia opinión sobre el control interno vigente en su área;

• La AI tiene que monitorear qué hace la Gerencia frente a las recomendaciones que se les hacen llegar: es indiferente ? es proactiva? o simplemente cumple porque no tiene más remedio pero sin convicción;

• El entorno de control existe?

f) SOX (Sarbanes - Oxley Act): Su cumplimiento permite que el Rol del AI se amplíe. Ha habido una gran inversión de dinero de las Empresas y mayormente, todos los esfuerzos están dirigidos en el último tiempo a la implementación de la Sección 404. Uno de los desafíos interesantes que se avecinan es cómo optimizar el Rol del AI a través de SOX. En estos momentos, se está estudiando la necesidad de hacer ajustes a dicha Sección, ya que profesionalmente se han levantado voces acerca de lo burocrático y lento del proceso de identificación de los puntos de control y la comprobación sobre si el control está trabajando o no.

g) Finalmente, voy a tomar como propio una máxima de Betty McPhilimy - Presidenta del Consejo de Dirección del IIA -: "APROVECHEMOS EL MOMENTO..... Este es un buen tiempo para ser auditor interno". Nuestro status quo se está elevando y nuestro papel dentro de las Organizaciones está cambiando, ya que hay una nueva realidad que afecta nuestro destino.

El futuro es bueno, sin duda.

3) Comité de Standards (IASB):

Se han desarrollado los siguientes temas: a) La conveniencia de la implementación de las Normas Standards y de poner Focus en su promoción; b) Prácticas para el desarrollo de las auditorías de calidad; c) Necesidad de que los miembros del Comité participen en Conferencias, hablando sobre los Standards. Asimismo, se definieron Grupos de Trabajo para abordar los siguientes tópicos: Risk Management Standards Review, Promotion of the Standards y Ética y Fraudes.

Quedo a disposición, Cordialmente.

Guillermo Reymundo Martínez
Presidente IAIA

Autor: Guillermo R. Martinez

Reforzando la seguridad
El proceso de mantener una efectiva arquitectura de seguridad

"***Seguridad no es una iniciativa sino un proceso que debe responder a las necesidades de la organización y debe ser mantenida mediante una continua evaluación***"

Segunda Parte

¿Qué significa entorno de arquitectura de seguridad?
Comencemos desde el ciclo más superficial:

- Gente, procesos y tecnología son las estructuras básicas de las organizaciones, siendo la más crítica la gente. La gente usa la tecnología para la construcción de procesos de negocio, por lo tanto estableciendo la interrelación entre las tres.

- Trabajamos con gente y a través de procesos y tecnologías para control, seguridad y mejora de sus entornos.

- La infraestructura es diseñada a través de tres fases del proceso - Estado Actual, Estado Deseado y Mejoras

- Cada una de las tres fases es usada para revisar los principales puntos de la seguridad en las políticas y procedimientos, tecnología y recupero y restauración.

- Luego la infraestructura nos lleva al segundo y tercer punto, aplicando las tres fases: Estado Actual, Estado Deseado y Mejoras.

- Con la primera fase del proceso, el análisis del estado actual y el grado a obtener es desarrollado.

- Mediante el cambio de parte de las personas, procesos o tecnología (y lo que es estático del entorno) el impacto caerá en seguridad en las áreas de Política y procedimientos, tecnologías y recupero y restauración.

- Los impactos en seguridad ante cambios en el entorno son difíciles sino imposibles de aislar.

- Con la segunda fase, se desarrolla un estado mejorado de infraestructura que es robusta y escalable.

- En la fase tres, el estado mejorado de seguridad es implementado e integrado para encontrar el entorno cambiado y las necesidades de la empresa.

En muchas empresas la función de tecnología informática ha evolucionado y crecido a través del tiempo, liderando o esperando cambios dentro de la organización. Mientras el desarrollo de una correcta arquitectura de seguridad debe corresponder a la situación actual de la organización, también necesita estar preparada para un estado innovador cuando sea apropiado.
Vemos un espectro de practicas dentro de tres áreas de arquitectura de seguridad: Políticas y Procedimientos, Tecnología, y Recupero y restauración. Con estas tres áreas, el corazón de la innovación es el impacto de Internet y los sistemas para acomodar el amplio entorno computadorizado y el entorno virtual según se puede apreciar en la figura 5.

En el intento de desarrollar una arquitectura amplia de seguridad de la empresa, es opinión de CTG que la organización debe determinar si está dentro de algunos de los puntos a continuación:

Políticas y Procedimientos	**Convencional**	**Creativa**
Comunicación de la información	Basada en papel: • Manuales y libros • Los cambios se distribuyen manualmente	Basada en la WEB (red): • De actualización instantánea • Disponible en toda la organización
Programa de concientización de seguridad	Orientación: • En el momento de la incorporación • Como único evento	Educación continua • Entrenamiento continuo • Como parte del negocio diario
Operaciones	Departamental • Sitio individual o en varios edificios • Mira las unidades de negocio como operaciones aisladas	Abarca toda la empresa • A través de todas las unidades de negocio • Considera las Inter.-dependencias entre las distintas unidades de negocio
Infraestructura	**Convencional**	**Creativa**
Sistema operativo	Desarrollado comercialmente: • A través de un proveedor (IBM) • Dificultad para intercambiar información	Sistemas abiertos: • Conexiones sin cable de operaciones a usuarios • Facilita el intercambio de datos entre plataformas
Aplicaciones	Puntos de solución • Aplicaciones para determinados procesos: Cuentas a Pagar, Cuentas a Cobrar.	Plataformas integradas • A través de toda la empresa - SAP, Oracle • Único punto de ingreso

		de datos
Acceso remoto	Discado • Punto a punto • Ancho de Banda limitada	VPN/ATM • Acceso virtual • Ancho de banda ilimitada
Integración de usuarios	Identificación de usuarios / Contraseña • Múltiples identificaciones y claves para cada sistema y plataforma	Servicios de directorio • Única identificación de usuario y clave para todas las plataformas y sistemas
Administración de datos	Base de datos • Bases de datos individuales • Debe conocerse donde radica la información	Repositorio de datos • Permite almacenamiento masivo de datos • Utilitarios de explotación de datos y generador de reportes
eCommerce	Fax • Manual • Múltiples puntos de contacto y manejo	Portal web • CRM • Intercambio de información inmediata
Tecnología	Centralizada • Distribuida entre unidades de negocios	Virtual • Los usuarios son independientes de su ubicación física • Múltiples puntos de acceso
Control y supervisión	Manual • Revisión de reportes de actividad • Ocupación intensiva	IDS • Automatizado • 24 hs. los 7 días de la semana
Recupero y restauración	**Convencional**	**Creativa**
Tecnología	Proveedor • Depende de un proveedor de back-ups	Interno • Superposición interna • Autosuficiente
Espacio	Espacio disponible • Dependiente de un tercero que tenga espacio disponible • Puede no ser adaptable a un entorno de trabajo • Focalizado en la pérdida de una única estructura	Triangulación • Autosuficiente • Operacional • Superposición prevista en la operación diaria • Reasignación de trabajos
Procesos de negocios	Espacio disponible • Depende de la disponibilidad de un tercero • Puede no ser adaptable a un entorno de trabajo	Oficinas virtuales • Fuerza de trabajo virtual o a través de celulares • En cualquier lugar y en cualquier momento
Planeamiento de reemplazos	Gerencia ejecutiva • Focalizado en la pérdida de un nivel "C"	Departamental • Incluye alta y media gerencia
Planeamiento de contingencias	Centro de datos • Se concentra sólo en el recupero y restauración de equipos y programas	Abarca a toda la empresa • Se concentra en la recuperación y restauración de las operaciones del

		negocio

Comprendido dentro de la metodología CTG's SAF está el proceso de evaluación de riesgos, tal como se describe en la figura 6. A través de la identificación de amenazas y vulnerabilidades, estaremos en condiciones de determinar el mejor foco de nuestra atención.

La siguiente es una breve descripción de cada una de las principales fases del proceso de evaluación de riesgos:

Captura del proceso:

- Identificación de Principales procesos críticos y claves (de información, físicos y funcionales) y sus dependencias de otros.

- Identificación de todos los componentes de infraestructura que son requeridos para soportar los distintos procesos.

- Identificación de propietarios, responsables de mantenimiento y consumidores de los componentes de los procesos y de infraestructura identificados.

- Ayuda en la ubicación de valor (imputado o intrínseco) y la importancia de los procesos y activos críticos y claves.

Evaluación de las amenazas:

- Identificación y asignación de importancia a aquellas amenazas que pueden llegar a afectar la organización.

• Cuantificación de la importancia que puede tener la amenaza para la organización.

• Cuantificación de la motivación y posibilidad de la amenaza.

Análisis de vulnerabilidad:

• Identificación y asignación de importancia a las vulnerabilidades conocidas asociadas con los procesos, activos y los componentes de la infraestructura específicos del cliente.

• Las vulnerabilidades son dirigidas a través de la definición completa del sistema durante el proceso de captura.

• Determinación sobre la posibilidad de que la vulnerabilidad pueda ser explotada física o electrónicamente.

• Medición del grado de severidad de la vulnerabilidad a través de la cuantificación de:

• daño potencial de la explotación de la vulnerabilidad

• anticuación de la vulnerabilidad (cuando fue descubierta)

• cantidad de información disponible sobre la vulnerabilidad

• determinación de los aspectos operacionales que son afectados por la vulnerabilidad

Determinación del riesgo:

Riesgo es la combinación de la amenaza afectando alguna vulnerabilidad que puede causar daño a un proceso o activo basado en la amenaza, vulnerabilidad y medición del activo previamente definido.

• Determinar qué amenazas pueden afectar qué vulnerabilidades contra los activos y procesos.

Evaluación de las contramedidas:

• Identificar las contramedidas aplicables considerando las amenazas específicas a la infraestructura, vulnerabilidades, procesos/activos y componentes.

• Producir una lista de contramedidas válidas para justificar el análisis de decisión.

• Factores de la contramedida están basados en:

• Factores de Procesos/activos: sensibilidad, nivel de criticidad, perdurabilidad, recuperabilidad, cantidad, calidad y valor económico.

- Factores de amenaza: acceso físico, acceso electrónico, posibilidad y motivación.

- Factores de vulnerabilidad: daño potencial, información disponible.

- Conducir un cálculo para mitigar el riesgo mediante la aplicación de contramedidas al factor de riesgo que éste mitiga.

Análisis de justificación de decisión:

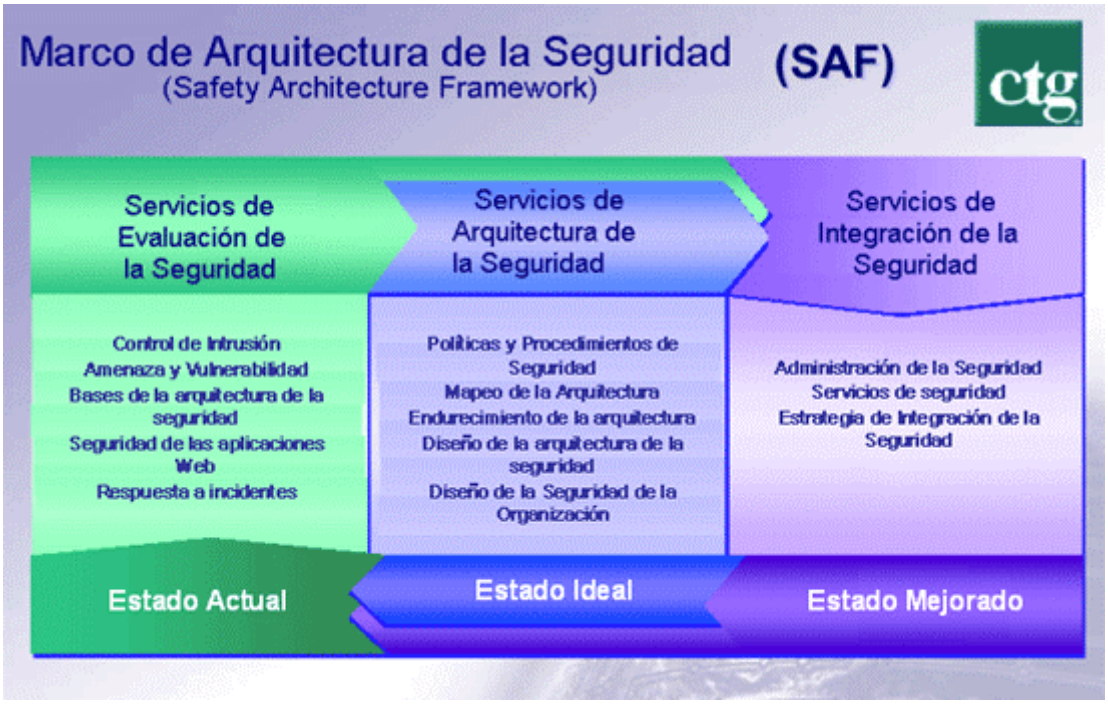
- Conducir un análisis de costo-beneficio:

    - Identificando grupos de soluciones comparables
    - Identificando la solución más eficiente en términos de costo
    - Considerando el índice costo/beneficio:

        - Riesgo Delta/costo
        - El mayor índice de costo beneficio implica la más efectiva solución
        - Identificar la solución que abarque más beneficios

- Para que una medida sea considerada debe mitigar al menos un factor de medición de riesgo.

La metodología CTG's SAF se concentra en el modelo establecido de Gente, Proceso y Tecnología y define servicios dentro de cada una de las tres etapas de la arquitectura de seguridad: Estado actual (evaluación); Estado ideal (arquitectura); y estado mejorado (integración). La figura 7 provee una representación gráfica de la metodología SAF y su flujo continuo desde el estado actual hacia el ideal y el mejorado para luego retornar al estado actual mostrando la necesidad de un monitoreo continuo y una evaluación del estado de seguridad.



CTG's SAF es un entorno que asegura consistencia, enfoque unificado para evaluar a la organización, validar y mejorar la posición de seguridad en general. SAF se concentra en la mitigación de riesgo asociados con el desempeño de las operaciones del negocio y su relación con la gente, los procesos y la tecnología. En la evaluación de la efectividad de la seguridad, SAF considera las políticas y procedimientos, controles de información y tecnología y la recuperación y restauración en cada una de las tres etapas.

CONCLUSIÓN

Seguridad implica asumir un nuevo rol dentro de la economía global y los mercados, como un facilitador de negocios. No debe implicar más un costo, su verdadero valor está siendo reconocido en la medida que les permite expandir sus mercados asegurando la disponibilidad, integridad y calidad de la información. Pero la seguridad no puede ser vista por la alta gerencia como un dispositivo a ser instalado o una política a ser implementada. Debe ser reconocida como una estrategia y un arma táctica en el campo de los negocios. Para ser efectiva, la seguridad debe ser integrada en todos los aspectos de las operaciones de la organización desde la protección del personal hasta el acceso remoto a las redes internas. El monitoreo continuo y la validación de barreras de seguridad y controles son el único camino para asegurar que no están siendo atacadas y que aún proveen el nivel de control requerido. El desarrollo y la integración de arquitecturas de seguridad que abarquen a toda la empresa requiere de la asistencia de toda la organización y el entendimiento de cada individuo de su rol y responsabilidad con relación al uso, protección y control de la información de la compañía y sus recursos tecnológicos.

Autor: Scott D. Ramsey

Los estandares de conducta y el buen gobierno corporativo

Definir procedimientos, políticas, códigos de ética es muy fácil; lo difícil es hacer que esos procedimientos, políticas y códigos se cumplan. Siempre hay una diferencia o un espacio entre lo que se espera de las conductas de los empleados y directivos, establecido en los procedimientos, políticas y códigos y la verdadera conducta demostrada por los directivos y empleados. Eticamente hablando, esa diferencia o espacio entre lo que se quiere y lo que realmente se obtiene, es conocida como la Brecha de Estándares de Conducta.

¿Qué es la Brecha de Estándares de Conducta?

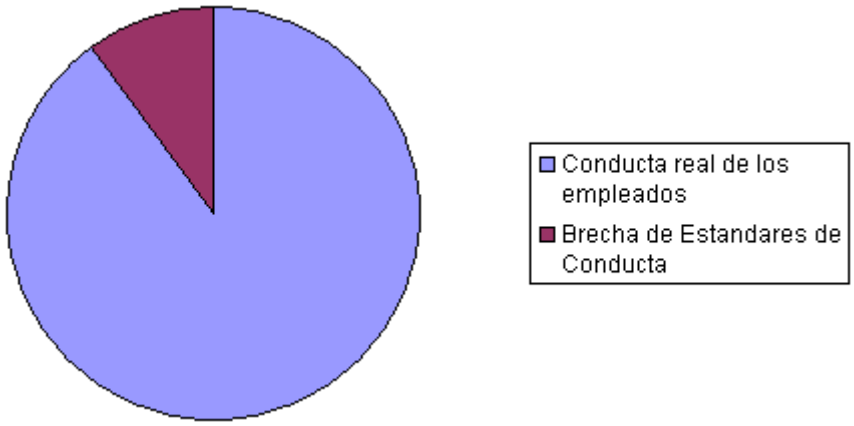
¿Si existe un reconocido problema, una crisis legal, una baja productividad, o un asunto relacionado con la calidad del producto, en su organización, usted lo ignora? Por supuesto que no, pero en muchas compañías un peligro no reconocido, amenaza en una proporción igual o mayor, no sólo las utilidades sino la salud corporativa en general. El peligro es la Brecha de Estándares de Conducta, que es la diferencia entre los estándares articulados por una compañía (en un código de conducta, en las políticas, y en los procedimientos) y la conducta de sus empleados. Esta diferencia erosiona la integridad, socava aún los mejores estándares establecidos y permite la conducta poco ética hasta convertirse en la norma general. Con la pérdida de la integridad se incrementa el riesgo financiero y reputacional, haciendo una organización vulnerable en términos de obligaciones legales y disminuyendo la confianza del consumidor y del inversionista. Sin embargo, la fuente de este riesgo, la Brecha de Estándares de Conducta, a menudo se ignora o no es reconocida.

En términos matemáticos, la ecuación de la Brecha de los Estándares de Conducta sería la siguiente:

B=Cd-Cr

O sea Brecha (B) = Conducta deseada (Cd) (la establecida por los códigos) - Conducta real de los empleados (Cr)

En el siguiente gráfico, se muestra también la Brecha, donde la totalidad del círculo es la conducta deseada y la otra parte es la conducta real de los empleados:



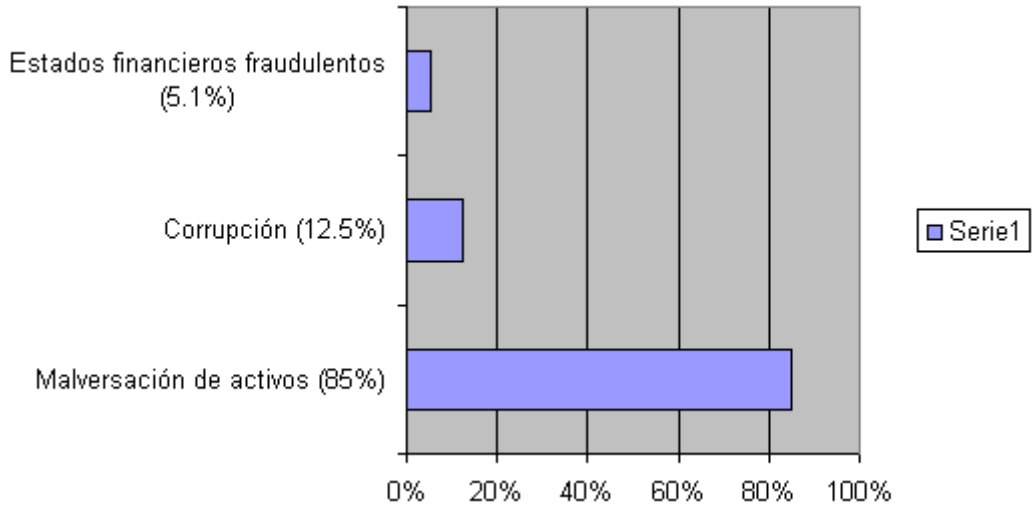
El problema no es con los estándares, es con la conducta. Establecer los estándares es la parte fácil. Enron, por ejemplo, tuvo un código de ética, entrenamiento en el cumplimiento de

las normas y un departamento de Responsabilidad Social. Enron de hecho tuvo claros los estándares que obligaban a tener certeza en sus registros financieros. Sin embargo, en muchos esfuerzos de reforma corporativa el enfoque ha estado en desarrollar estándares sin un énfasis similar en comunicar y modelar las conductas que demuestran esos estándares. Las acciones de los líderes de Enron contradijeron sus estándares, y en esa brecha entre las conductas y los estándares, se perdió una compañía.

Ha llegado a ser común desechar la lección de Enron, para indicar con mucha confianza de ***"que eso no podría suceder aquí."*** La Brecha de Estándares de Conducta existe en cada compañía, porque ninguna organización, ni los empleados ni el director son perfectos. La única pregunta verdadera es: ***qué tan ancha es esa brecha?*** , y ***esa brecha, qué nivel de riesgo tiene en su compañía?*** . Un estudio de 2002 hecho por la Asociación de Examinadores Certificados de Fraude (Association of Certified Fraud Examiners) identificó tres tipos primarios de fraude financiero: malversación de activos, la corrupción, y los estados financieros fraudulentos. El tipo más común de fraude, malversaciones de activos ocurrieron en el 85 por ciento de las compañías encuestadas con un costo promedio de $80,000 dólares. La corrupción se presentó en el 12.5 por ciento de las compañías encuestadas, con una pérdida promedio de $530,000 dólares. Los estados financieros fraudulentos aunque fueron menos comunes (ocurrieron sólo en el 5.1 por ciento de los encuestados), la pérdida promedio por ese fraude fue de $4,250,000 dólares.

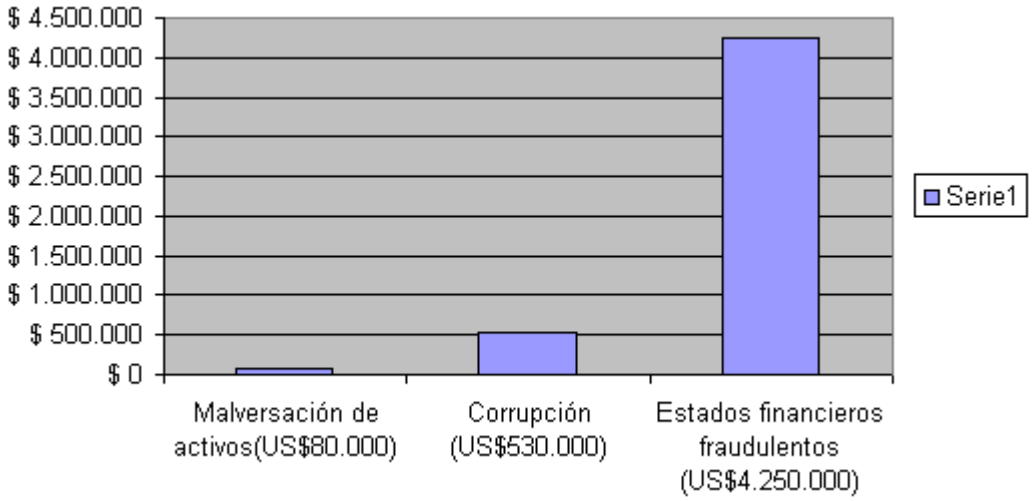
FRAUDE FINANCIERO

(En términos de porcentaje)



FRAUDE FINANCIERO

(En términos de dinero (US$))



Hemos visto que los riesgos van aún más allá del caso Enron: TAP Pharmaceuticals fue multada con más de $840 millones por inflar artificialmente el costo al por mayor de una droga contra el cáncer, para proporcionar más incentivos a las utilidades para los médicos y a los sistemas administrados de asistencia médica (que sería reembolsado por los seguros médicos (Medicare y Medicaid)) por prescribir la droga.

Credit Suisse First Boston está bajo investigación por la Asociación Nacional de Distribuidores de Valores (National Association of Security Dealers) en 2002 por un proceso conocido como "spinning," que es ofrecer determinados IPOs (Initial Public Offering - Oferta Inicial Pública) a clientes específicos favorecidos a cambio de recibir negocios para el grupo de inversiones del banco. Esta investigación ya ha llevado a determinar cargos de obstrucción a la justicia para el ejecutivo encargado.

Hemos visto también los efectos devastadores de ignorar la Brecha de Estándares de Conducta en los empleados. Bob Boles de Cartersville, Georgia, fue suspendido de su trabajo de soporte técnico en WorldCom. Lo qué él le dijo a NBC News ilustra el aumento de la conciencia: *"En 16 años de sangre, sudor y las lágrimas, yo viví y respiré la compañía. Cuándo este escándalo de contabilidad salió a la luz pública y el precio de las acciones golpeó el piso, mi plan de jubilación, que en un punto valía casi $250.000 dólares, ahora no vale más que 10 centavos,"* dijo. *"Yo estoy devastado. Estas personas tienen que ser encontradas responsables."*

Mientras todas estas organizaciones tenían los estándares implementados, el enfoque principal no era si no había un espacio entre los estándares y la verdadera conducta y si ese espacio había creado los riesgos. Cuando las experiencias de estas compañías y de otras ilustran, que establecer los estándares no es suficiente y que si los empleados no los siguen, la organización encara enormes riesgos. Por el propio bien de las compañías, de los empleados y de los inversionistas, la Brecha de Estándares de Conducta debe ser establecida.

¿Por qué existe la Brecha de Estándares de Conducta?

La Brecha de Estándares de Conducta puede desarrollarse por varias razones. En su origen es a menudo una equivocación por parte de los líderes de la organización, de la relación que existe entre los estándares y la conducta. Los líderes pueden creer, por ejemplo, que porque se ha establecido un conjunto de reglas, los empleados naturalmente las seguirán. La realidad es que hacer las reglas es sólo un primer paso, y que los estándares por sí sólos, no pueden garantizar la integridad.

El elemento crítico para disminuir la Brecha de Estándares de Conducta es el ambiente de control de la compañía, que es la base de la cultura corporativa. El ambiente del control es el contexto en el cuál son tomadas las decisiones y fija los parámetros para la organización entera. Esto comprende las actitudes, las habilidades, la conciencia y las acciones de los empleados de la compañía, especialmente sus líderes. Últimamente, un escaso ambiente de control es el responsable del aumento de la brecha entre los estándares de la organización y la manera como se comportan sus empleados. Para entender cómo el ambiente de control afecta la conducta, es importante entender la importancia del contexto. La conducta ética (o poco ética) no existe en un vacío, pero forma parte de una cultura organizacional más amplia que se desarrolla con el tiempo.

El Poder del Contexto

Los modelos más viejos de organizaciones están enfocados en la conducta individual. Se asumió que según la inclinación natural de empleado, éste debía actuar sólo en su propio interés, y por lo tanto necesitaba una vigilancia estricta. El pensamiento inclusivo y más contemporáneo se enfoca en el ambiente en el cuál el individuo actúa. Incluso aún las buenas personas son susceptibles a influencias negativas del ambiente. Por ejemplo, en su libro, "The Tipping Point," el autor Malcolm Gladwell discute lo que él llama *"el poder del contexto"* en términos de los estudiantes que hacen trampa en los exámenes de la escuela. El descubrió que algunos estudiantes, nunca harán trampa. Otros siempre tratarán de obtener un margen poco honrado. Para la gran mayoría, la sección más grande de la curva de la campana de la clase, hará o no hará trampa de acuerdo como lo determine el ambiente del aula (su *"ambiente del control"*). La poca supervisión y la percepción de que no hay ningún castigo, por ejemplo, alentará a más estudiantes a copiar las respuestas de los exámenes de sus compañeros, mientras las condiciones opuestas parecen obligar a lo que llamaríamos la honradez. Claramente, una característica que podemos haber creído, forma parte de que el carácter innato de una persona es influenciada por el contexto.

La importancia del contexto se ilustra mejor en el temor de la venganza. La mayoría de las conductas poco éticas ocurren no a causa de una ganancia personal, sino porque los individuos piensan que esa conducta es necesaria para mantener sus trabajos. En WorldCom, la jefe le solicitó a Betty Vinson que hiciera registros contables falsos. Al principio ella se negó. Pero luego ella cedió a la presión. Durante seis trimestres ella hizo los registros ilegales para aumentar las utilidades de WorldCom. Al final de 18 meses, ella ayudó a falsificar por lo menos $3.700 millones de dólares en utilidades para mantener su trabajo. El contexto, el ambiente de control, ayudó a la conducta poco ética de los líderes de WorldCom, a pesar de que Betty Vinson, quiso hacer las cosas correctas.

La cultura corporativa como un Factor de Riesgo

Las debilidades en una cultura corporativa o en el ambiente de control aumentan el riesgo y crean la Brecha de Estándares de Conducta. Tales debilidades incluyen:

La falta de liderazgo y visión: La ausencia de un liderazgo fuerte en una organización tendrá como resultado, una falta de modelos de roles para los empleados de la organización. Si los líderes no *"hacen lo que dicen"* y modelan la conducta deseada, entonces no pueden esperar que los empleados se comporten apropiadamente. La falta de liderazgo puede ser también manifiesta en una falta de visión. La falta de una visión clara de los objetivos de la organización y de prácticas éticas apropiadas crea un ambiente de control que probablemente aumente la brecha entre los estándares y la conducta. Sin la visión, por ejemplo, es difícil establecer los estándares apropiados: si las reglas de conducta son inalcanzables esto desalienta a los empleados y si son demasiado laxas no presentan un desafío para ellos. La falta de visión también puede tener como resultado la apatía. Los líderes que no se pueden comunicar y que no pueden demostrar un compromiso con la integridad, posiblemente no lo pueden inculcar en otros.

Comunicación pobre: La incapacidad para comunicarse efectivamente puede socavar la posición ética del ambiente de control, fomentando aún más una falta de claridad, mensajes ambiguos, y la incapacidad para entregar malas noticias. Sin claridad, no se puede esperar que los empleados entiendan lo qué son los estándares y cómo se deben comportar. Los mensajes ambiguos confunden aún más a los empleados comprometidos con acciones y respuestas correctas, y la incapacidad para comunicar las malas noticias significa que la aplicación y los resultados nunca serán concretos para los empleados.

La presión indebida para actuar: La presión descontrolada o poco realista para producir resultados pueden aumentar también la brecha. Si el ambiente del control coloca un énfasis indebido en los resultados, sin tener en cuenta la integridad, alentará a los empleados a tomar atajos, arriesgándose e incluso alentando la conducta poco ética. En un ambiente competitivo, la administración debe tener cuidado para no alentar la creencia de que *"se puede hacer cualquier cosa,"* en otras palabras, que es aceptable para los empleados romper las reglas para obtener una utilidad rápida. Tal desequilibrio en las prioridades arriesga la salud corporativa a largo plazo por las ganancias a corto plazo.

La falta de acceso: A los empleados se les debe proporcionar canales establecidos de comunicación que les permita pedir ayuda con los dilemas éticos y a través de los cuales, ellos puedan informar las violaciones éticas. La falta de tales canales envía el mensaje que esa administración no quiere oír sinceramente acerca de las preguntas ni de los problemas e incluso los empleados éticos pueden decidir no tomar el paso extra para preguntar acerca de un problema o de emitir un reporte.

El temor de la venganza: El despedir a los *"soplones"* (los que informan la conducta poco ética, como sucedió tanto en Enron como en WorldCom) aumenta la Brecha de Estándares de Conducta. Incluso los empleados éticos dudarán en informar la conducta poco ética o ilegal, si ellos temen que pueden perder sus trabajos a causa de eso.

La aplicación contradictoria: Reglas diferentes para diferentes empleados, reglas que cambian según la situación, y reglas que son aleatoriamente o raramente impuestas envían el mensaje que los estándares no son sólidos o que sinceramente no son valiosos para la compañía. Por ejemplo, cuándo Enron renunció a aplicar su propio código de ética a su gerente financiero, creó una cultura corporativa que claramente alentó la utilidad a corto plazo a costa de la ética y del verdadero crecimiento a largo plazo. En un nivel más pequeño, la ética de muchas culturas corporativas se socava cuándo los empleados ven que las reglas son diferentes para diferentes grupos de personas. Por ejemplo, los colegas que producen las utilidades, a menudo no son penalizados por *"tomar atajos,"* o asegurar esas ganancias a

través de maniobras poco éticas. Esta política *"de vista corta"* perjudica todo el lugar de trabajo y no ayuda pero en cambio si puede conducir a una moral más baja, al cumplimiento de una ética pobre, y a asuntos más graves a largo plazo.

La falta de educación, de herramientas, y apoyo: En muchas situaciones, el empleado no sabe cuál es la decisión correcta, o cómo actuar cuando se enfrenta con un cierto dilema. Una organización que no le da a los empleados las herramientas y el entrenamiento para respaldar la integridad en el proceso de toma de decisiones envía un mal mensaje. Una organización que desea fomentar un lugar de trabajo ético hará que se aprenda con las herramientas disponibles. Hará un esfuerzo de educar regularmente y vigilará la conciencia ética de sus empleados. Apoyará y recompensará el comportamiento ético e incrementará la conciencia de la ética como parte de su código regular corporativo.

Disminuir la Brecha de Estándares de Conducta

La clave para disminuir la Brecha de Estándares de Conducta es un proceso compuesto de dos pasos. Primero, los líderes de la organización deben identificar los factores específicos de riesgo que han creado y ensanchado la brecha. Entonces, la organización debe implementar un plan para mitigar y administrar ésos factores de riesgo. Al igual que con cualquier otro objetivo de negocios, los líderes deben enfrentar esta amenaza con una visión segura, con una planificación estratégica, y con un compromiso de cambio. Para cambiar realmente la conducta, los líderes necesitan comprometerse con un proceso de mejoramiento continuo.

Disminuir la Brecha de Estándares de Conducta debe también involucrar los procesos establecidos, las herramientas, la comunicación, y la educación progresiva para respaldar los estándares de la organización. Crear un libro de reglas no será suficiente, ni tampoco el hecho de tener una aproximación de *"arreglo rápido"* . Sólo aceptando la naturaleza progresiva de este desafío, las organizaciones pueden llevar la conducta del empleado a la par con los estándares de la organización.

Los beneficios de disminuir la Brecha de Estándares de Conducta son tres:

- Mejora la visión financiera;
- Mejora la reputación; e
- Incrementa la eficacia en un lugar de trabajo cada vez más competitivo.

Llevar la conducta más cerca a la par de la ética de la organización reduce mucho los riesgos financieros asociados con la conducta poco ética. Una organización que trabaja para disminuir la Brecha de Estándares de Conducta se beneficiará evitando multas punitivas a corto plazo, tal como los $840 millones de dólares de multas que pagó TAP Pharmaceuticals en el ejemplo dado anteriormente. Puede proporcionar también la protección contra el descenso del valor de las acciones.
Una organización que trabaja en disminuir la Brecha de Estándares de Conducta gana en términos de la percepción pública: una compañía que demuestra su compromiso con la integridad, y juega limpio dentro de su campo, es una compañía que será confiable para el público y para los inversionistas.
Johnson y Johnson hizo esto en 1982 cuando respondió a la crisis de Tylenol con integridad. Enfrentado a una horrible situación, (la introducción de cianuro en su producto popular había tenido como resultado la muerte de siete personas), la organización tuvo varias opciones. La compañía podría haber tratado de restar importancia a la crisis, quizás aumentando la

publicidad para incrementar la confianza del consumidor o definiendo la situación como un acto criminal aislado. Pero Johnson y Johnson escogió actuar ética y proactivamente, yendo más allá de lo realmente necesario para fortalecer la seguridad del consumidor. Actuando en su compromiso con los profesionales de la salud y los consumidores, la compañía suspendió la producción y la publicidad, retirando del mercado y destruyendo 31 millones de botellas de la droga sin receta con un valor de venta al por menor de más de $100 millones de dólares. Las acciones bajaron de precio tras el escándalo, pero se mejoraron a causa de esta respuesta proactiva. La conducta ética ha continuado pagando el precio, con el aumento de la confianza del consumidor que ha sido una constante durante más de 20 años.

Por el contrario, Firestone permitió que se erosionara una reputación de 100 años al final de la década de los noventa cuando rechazó una respuesta ética proactiva a los problemas con sus llantas Wilderness AT y ATX. Cuándo aparecieron los problemas, Firestone tuvo primero una oportunidad en la que podría haber actuado como lo hizo Johnson y Johnson, decretando una comprensiva retirada de sus llantas del mercado, extendiendo el programa para consolidar la seguridad del consumidor. Por el contrario, culpó a muchos otros de los problemas, por un mantenimiento inadecuado de las llantas y por los vehículos en que se instalaron las llantas. Pero luego en el año 2001, acordó retirar las llantas del mercado, con un cargo por una sola vez de $350 millones de dólares. Pero para entonces la compañía había llegado a ser asociada con accidentes por la explosión de las llantas y por problemas de seguridad que pueden aumentar este valor general en los años siguientes. Recientemente, en mayo de 2003, Firestone estaba todavía llegando a acuerdos judiciales por los pleitos relacionados con el retiro de las llantas del mercado.

Mejores Prácticas para Cambiar Positivamente la Conducta Corporativa

En un mercado global cada vez más competitivo, los líderes corporativos llegan a ser conscientes que los nuevos productos y las tecnologías no pueden seguir siendo tenidos en cuenta simplemente con ofrecer un margen competitivo. Cuando el mercado se reduce, el único margen seguro proviene del compromiso, de la participación, y de la responsabilidad de los empleados. Estas cualidades no son fomentadas por un libro de reglas; ellas provienen de una cultura corporativa orientada en valores que alientan y fomentan la conducta ética.

Para cambiar positivamente la cultura corporativa, las organizaciones deben utilizar todos sus recursos, empezando con dar a sus empleados, los instrumentos apropiados. Así como un editorial de la revista Fortune lo aconsejó, las corporaciones *"deben convertir a sus empleados en gobernadores corporativos"* comprometiendo todo el lugar de trabajo con el objetivo de tener un ambiente corporativo ético.

También los ejecutivos más jóvenes quieren ayudar: Una encuesta del Instituto de Aspen (Aspen Institute) recientemente le preguntó a estudiantes en 12 programas internacionales de MBA lo que ellos harían si encontraran que sus valores chocaran con los valores de la compañía que los empleó. Cerca de la mitad de los encuestados, (el 44 por ciento) dijeron que ellos tratarían de involucrar a otros empleados de la compañía para que se unieran para enfrentar esas preocupaciones.

Los empleados, también, están invirtiendo en la ética corporativa: la historia reciente en organizaciones tales como Enron y WorldCom han ilustrado el costo que tiene para los empleados la conducta poco ética, así como la mala conducta de la administración que ha causado que los empleados pierdan los trabajos y la seguridad financiera, en los planes

desvalorizados de jubilación financiados por acciones de la compañía, por ejemplo. El efecto de la ética corporativa en la seguridad del empleo y los ingresos futuros de la jubilación ha hecho sensibles a los empleados a la necesidad de tener un confiable y ético lugar de trabajo y les enseñó a aumentar el cumplimiento ético, que se mueve más allá de seguir pasivamente unas reglas.

Depende de los líderes conducir estas fuerzas potenciales teniendo una visión de integridad para la organización y un plan estratégico para asegurar tal integridad. Esta visión debe ser articulada de una manera que sea pertinente y procesable por los empleados; debe ser vista como inspiradora pero también alcanzable. Una visión muy alta no será tomada seriamente mientras que una visión muy baja no motivará a los empleados.

El plan estratégico que los líderes deben diseñar e implementar tiene que contener varios elementos. Para desarrollar la infraestructura que respaldará y estimulará la conducta ética, debe incorporar la comunicación, el entrenamiento y el desarrollo, y el mejoramiento del proceso de los negocios, que llevan a cabo la visión de la integridad. Creando esta visión y aplicando ese plan estratégico, los líderes pueden actuar como modelos de roles. Los líderes pueden hacer avanzar a la organización más allá de la ética basada en reglas a un mundo más global de ética basada en valores. Los líderes pueden crear un sistema que permita a los empleados a comprometerse activamente y a participar en una cultura corporativa ética.

Autor: Rene M. Castro