# El Rol del Oficial de Seguridad

**(Information Security Officer, ISO, Chief Security Officer ó CSO para los amigos)**

**Lic. Marcelo F. Rodríguez**
**MBA/CISA/PMO**
**mrodriguez at root-secure.com**
**Root-Secure Director**
**Fecha de Publicación: 09/04/08**

Sin temor a delatar mi longevidad, debo decir que ya llevo más de 15 años en el tema de Seguridad y no dejo de escuchar las mismas discusiones que oía allá por mis inicios:

¿El ISO debe Administrar Seguridad? ¿Debe controlar que se implementen las medidas recomendadas? ¿O simplemente debe decir qué hacer? ¿O ninguna de las anteriores…?

Pareciera que no hay Norma, Ley, Disposición o Circular que dé luz sobre el tema. Y las interpretaciones nos pueden llevar a tomar como válida cualquiera de las respuestas anteriormente dadas.

El hecho es que tampoco hay una respuesta lineal y única para todas las empresas. Cada una tiene su realidad y, por lo tanto, sus propias necesidades. Con lo cual el problema es aún mayor.

Entonces, ¿qué rol debe cumplir el ISO? Evidentemente, el que la Empresa demande.

No es la intención dar una respuesta universal al problema planteado. La propuesta es desafiar a cada modelo y así poder decidir conscientemente con cuál de los esquemas podemos salir a combatir más dignamente. Hacia allá vamos.

**El ISO como Administrador de Seguridad.**

Muchas instituciones tienen esto por Norma. Los Perfiles, Usuarios, Accesos y otros aspectos sumamente críticos, son administrados por un área de Seguridad de la Información independiente de TI.

Visto de otra forma, lo que antes podía hacer IT, ahora no puede (o se supone que no puede…), pero sí lo puede hacer el Oficial de Seguridad.

Por ejemplo, dar de alta un usuario, otorgarle privilegios, hacer un par de transacciones, eliminarlo, sacar un pasaje y partir hacia destino incierto, sin dejar rastro. Sospechas, muchas. Certidumbres…. Depende de la habilidad.

La pregunta que naturalmente surge es ¿por qué el ISO es más confiable que la gente de IT?

Supongamos que no se trata de un tema de confianza. ¿Es una cuestión de conocimiento y capacidades? Pensemos en la cantidad de cosas que se podrían hacer, desde las ya explicadas, hasta vender información. En mi opinión, hoy en día está más consciente un ISO que una persona de TI de las maravillas que se pueden hacer.

Pero veamos el tema desde otra óptica.

Supongamos ahora que nuestro ISO "Administrador" es muy celoso de su trabajo. Define una Política de Contraseñas con un mínimo de longitud de clave de 12 caracteres, que combine mayúsculas, minúsculas, caracteres especiales y números, no comience con 0 ni finalice con 08 (el año que viene se actualiza), que se deba cambiar cada 30 días, no repetir las últimas 12 y que sea distinta para cada Sistema (cualquier similitud con la realidad es pura coincidencia).

Pero tampoco escapa a los problemas Presupuestarios y de Recursos. Por lo tanto, se incrementa la cantidad de cuentas bloqueadas, los "blanqueos" de contraseñas y los Incidentes que debe investigar, pero con la misma cantidad de Recursos.

Y su subconsciente repitiéndole 24 horas al día "Si con 6 caracteres era más que suficiente!!!"

Es evidente que Definir y Administrar genera pérdida de independencia por problemas de Segregación de Funciones. La ventaja: la próxima vez lo va a pensar mejor, y los usuarios finales y IT, agradecidos…

Para colmo de males, la Compañía tiene Windows, Unix, Linux, AS/400, Oracle, MySql, un Solaris por acá, un Atala por allá y un sinnúmero de aplicativos existentes y por aparecer…

Analicemos este tema desde el punto de la Gerencia General o el Directorio, que deberían ser los principales interesados y son sin duda los principales afectados.

Bajo un esquema de caeteris paribus, ¿se reduce el riesgo? Si Uds. fueran el Director Financiero, ¿se irían a dormir tranquilos?... Pasemos a otro tema.

**El ISO como "Auditor"**

Para esto vamos a comenzar desde el principio. En 1985 aparece el primer estándar internacionalmente reconocido de Control Interno: el Informe COSO. Ya en ese momento se establece que el Control Interno **es** responsabilidad de la Gerencia y **no** de Auditoría.

Si no se cumplen los Controles establecidos por el Directorio o Gerencia General a través de la Política de Seguridad y sus derivados, no es responsabilidad de Auditoría y mucho menos del ISO. Es responsabilidad de la Gerencia.

Obviamente, si el ISO no ha desarrollado nada al respecto, ya las responsabilidades son dudosas. No se puede pedir control sobre lo que no está definido o normado.

Pero igualmente insistamos sobre el tema y, desde la óptica del Directorio o la Gerencia General, hagámonos la siguiente pregunta:

Si el ISO Define y Audita, ¿Quién me asegura que el ISO esté haciendo lo correcto?

Salvemos esta situación, un tanto engorrosa, con una Auditoría Interna o Externa que audita al ISO. Y ya que está, ¿por qué no audita el resto también? Es como que el tema se potenciaría.

Pero igualmente insistamos.

¿Cómo vamos a ver a los Usuarios? ¿Cómo quién viene a recomendarles mejoras para el cuidado de la información o a obligarlos a implementar controles, sobre los cuales luego los va a auditar quien los obliga?

¿Cómo nos verán los Usuarios? ¿Cómo alguien a quien hay que contarle para que los ayude o como alguien a quien si le cuentan cometen un acto de SINCERICIDIO? (si, está bien escrito. La Real Academia Española debería incorporarlo, si no lo hizo ya!!!!)

Si sumamos a la pérdida de independencia, el rechazo por parte de la Organización, este esquema no suena muy apetecible.

No cabe duda alguna que si la Auditoría no existe o no es muy hábil en la materia, alguien debería hacerse cargo de esto.

Dos utopías al respecto:

1. Entrenar a la Auditoría Interna si la hay.
2. Que sea las mismas Gerencias que determinen como se va a Controlar ante la ausencia del amado auditor. Si en definitiva son ellos los responsables del Control.

Y si no hay mas remedio, convivir lo mejor que se pueda con ambos sombreros.

**El Rol del Oficial de Seguridad**

Insistamos con las fuentes, pero esta vez extrayendo dos párrafos de la ISO 17799:2005 y veamos si nos puede dar un poco de luz sobre el tema.

*"Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement."*

Existe una diferencia importante entre Auditar e Implementar un Sistema de Medición para Evaluar y "**Sugerir**" mejoras. El inglés es un idioma conceptualmente muy preciso.

Pero esto no es todo.

*"In many organizations an information security manager will be appointed to take overall responsibility for the development and implementation of security and to support the identification of controls.*

*However, **responsibility for resourcing and implementing the controls will often remain with individual managers**. One common practice is to appoint an **owner** for each asset who then becomes responsible for its day-to-day protection."*

Ups!!!! Como se le parece al Informe COSO!!!!

En una oportunidad, en una reunión de Comité Ejecutivo de una empresa, se definió el rol del Back-Office (todo lo que soporta el Negocio), donde estaba incluida el área de Seguridad de la Información, de la cual estaba a cargo. Esta definición me fue de una ayuda enorme, y por esto quiero compartirla:

“En un barco están el Capitán, el Timonel, los Marineros, Maquinistas, Artilleros, Médicos, Cocineros, etc. Pero hay un rol y una función que muy pocos conocen: **El Navegante**.

Su tarea consiste en leer las cartas de navegación, saber la ubicación actual exacta, ver el clima, el estado de los motores, el estado general del Barco, de la tripulación y fundamentalmente sabe donde está el Puerto al que se quiere llegar (Estrategia), el camino que se quiere seguir (Táctica), el Tiempo (Objetivos) y en que Estado se quiere llegar (Valores).

Su función: entender los Riesgos a los que está expuesto el Barco, que pueden impedir su llegada a destino en las condiciones planteadas.

**E informar de esto al Capitán, para que pueda tomar la mejor decisión”**

El Tripulante no va en el timón, no está en las máquinas ni limpiando la cubierta. No toma las decisiones, sino que es parte integral del proceso de Toma de Decisión del Barco.

En mi opinión personal, éste es la principal función del ISO. Ayudar a la Gerencia a evitar las amenazas que les impidan lograr los Objetivos planteados. No a evitarlas por ellos.

El método: Conociendo claramente los Objetivos del Negocio, sus Estrategias, Tácticas y Valores. Y realizando un Análisis de Riesgos a partir de ellos, involucrando en él a la Gerencia.

El resultado: **la decisión correcta.**

Pero volvamos a la cruda realidad. Nada es así de perfecto.

Hay algo que es totalmente cierto. Estamos para cuidar el Negocio.

Y permanentemente oigo hablar de Firewalls, VPN’s, Vulnerabilidades, Ataques, Exploits, Logs. Excepcionalmente escuché a un colega hablar de Participación de Mercado, Crecimiento, Rentabilidad, Cash-Flow, Posicionamiento de Marca, y todos estos factores que son la base fundamental del Negocio.

¿Cómo podemos proteger adecuadamente algo que no conocemos y mucho menos entendemos?

¿Y cómo podemos hacerlo sin contar con la estructura adecuada?

En mi modesta opinión, hay que lograr tres pilares fundamentales sobre los cuales apoyarnos:

1. Definir que se quiere hacer y medir lo realizado (Comité e ISO)
2. Hacer lo que se debe hacer (Dueños de Datos, Usuarios y TI)
3. Verificar en forma independiente si se ha hecho bien (Auditoría)

Como todo, si uno de estos pilares se debilita o no existe, hay que reforzar los otros dos para que la estructura no se desmorone. Pero sin duda va a quedar más débil y va ser más costosa.

Lo importante: reflexionar sobre dónde estamos, y determinar las causas de nuestros males. Y a partir allí, hacer lo mejor que podamos. O tal vez estemos fantástico donde estamos…

Atreviéndome a extraer un párrafo de la obra ***Edipo Rey*** de Sófocles, cuando Tiresias, un ciego adivino, responde a una acusación de Edipo:

***"Y te digo, puesto que ahora me has ultrajado de ser ciego, que tú tienes y no ves en qué punde desgracia estás, ni dónde habitas, ni con quién convives"***

Les deseo la mejor de las suertes!!!!!!