SGPI: Privacidad y beneficio económico en un SGSI

Por Agustín López Neira, auditor SGSI certificado por British Standards Institute e ITIL Foundation.
Co-editor de www.iso27000.es

Introducción

En el presente artículo analizamos los factores clave que suelen determinar el modo en que se acepta y aborda la implantación y mantenimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI).

El análisis muestra el motivo de algunos de los errores más frecuentes y se presentan argumentos de negocio, de especial interés para la alta gerencia, que tratan de evitarlos. El objetivo final es ofrecer una visión más clara de los beneficios económicos y garantizar, definitivamente, la implantación decidida de los SGSIs en las empresas.

Para una mejor comprensión de las ideas fundamentales que deseamos transmitir introducimos por primera vez, y de forma original, lo que hemos venido a denominar *SGPI* en referencia a un *Sistema de Gestión de la Privacidad de la Información* y que presentaremos a continuación.

Considerar la gestión adecuada de la privacidad a partir del establecimiento de un SGSI permitirá una exposición más clara de los beneficios económicos que pueden obtienen las empresas y demuestra ser la llave adecuada que abre la puerta a la explotación de nuevas oportunidades de negocio.

Gestión de la Seguridad

Desde los distintos medios de información se destaca persistentemente que la información se ha convertido en un activo vital para el desarrollo y la continuidad de negocio de cualquier organización.

La protección adecuada de la información en las empresas debería considerar aspectos organizativos y tecnológicos, examinando como las personas utilizan los activos de información y los recursos en el desempeño de su trabajo diario. Esta evaluación es de vital importancia para poder disponer de unas líneas básicas de referencia e introducir mejoras que demuestren ser efectivas.

Sin embargo, la búsqueda de soluciones aún se centra exclusivamente en la compra directa de unos productos técnicos que se muestran invariablemente incapaces de cubrir todos los aspectos necesarios para alcanzar, por si mismos, los niveles de protección necesarios.

Como consecuencia, considerando además el aumento generalizado del número y variedad de las amenazas, es lógico concluir que los presupuestos que se dedican internamente a la seguridad nunca parezcan ser suficientes.

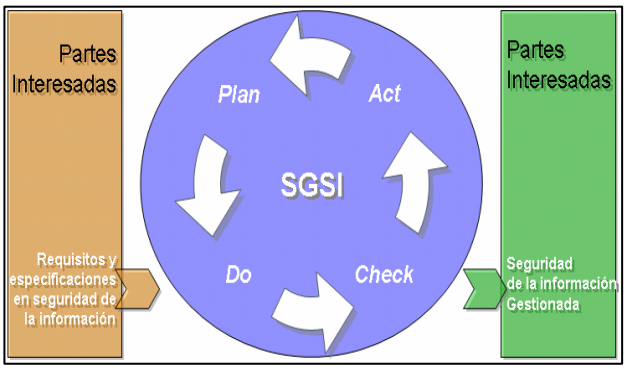
Pero debemos tener presente que una empresa no se dedica a los negocios para ser segura sino para ser una empresa que obtiene beneficios.

Es obligado, por tanto, establecer la apropiada relación entre los objetivos de negocio y los problemas en seguridad que afectan a estos objetivos, si es que la empresa tiene la intención de evitar realmente el consumo de tiempo y dinero en sus propios esfuerzos en seguridad.

Eludir esta relación y la adopción de una sistemática que demuestre la efectividad de las medidas que se adoptan conduce a, inevitablemente, alcanzar niveles de gestión de la seguridad y actualización insuficientes que carecen de controles básicos y elevan el número de fraudes, fugas de información, abusos e incidentes posibles.

Gastos extraordinarios o inesperados, juicios legales por incumplimiento de obligaciones y responsabilidades contractuales, cese parcial o total de las actividades, falta de servicios o niveles de disponibilidad inapropiados para seguir la dinámica y evolución de los mercados o ausencia de medidas de contingencia y planes de continuidad para superar situaciones inesperadas son algunas de las principales consideraciones que toda empresa debería saber cómo afrontar y evitar.

En relación a las obligaciones legales recordamos el riesgo a posibles sanciones que alcanzan hasta los 601.012,010 € en España. Los grados de aplicación quedan fuera de duda con la consulta de las resoluciones de procedimientos sancionadores, disponibles en la propia web de la Agencia de Protección de Datos.



Con el propósito de limitar la exposición de empresas y organizaciones a situaciones que comprometan la continuidad de sus actividades y beneficios, la norma ISO/IEC 27001 proporciona un modelo adecuado para establecer, implantar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información considerando las actividades y objetivos de negocio propios de cada organización.

El SGSI es un proceso armonizado con otras normas de difusión internacional como ISO 9001 e ISO 14001 y que puede alinearse fácilmente con sistemas de gestión de mejora continua en base al ciclo de Deming, comúnmente denominado PDCA (Plan, Do, Check, Act).

El objetivo fundamental del SGSI es asegurar la:

- Confidencialidad: acceso a la información por parte únicamente de quienes estén autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Para lograrlo, la organización necesita integrar políticas, personas, procesos y tecnología de modo que se permita el acceso de información a las personas adecuadas en el momento preciso dentro del contexto adecuado.

Todas las ideas fundamentales que hemos desarrollado hasta este momento captan la atención y suscitan el interés general en los SGSI.

Sin embargo, la exposición detallada del proceso completo de implantación descubrirá inevitablemente cuestiones relevantes que deberán ser resueltas con acierto para evitar serias dificultades en el proceso de aceptación e implementación y según los términos que propone ISO 27001.

Dificultades para la aceptación de un SGSI

Las dificultades aparecen durante la explicación del proceso de análisis de riesgos y vulnerabilidades y se intensifican con la necesidad de colaboración de una parte importante de las personas de la empresa con la dirección al frente.

Siguen con la lista de posibles controles aplicables que sugiere, en definitiva, gastos en mayor o menor medida y en relación a la formación, tecnología e infraestructuras, cambios organizativos, adopción de nuevos procedimientos y de gestión documental en la empresa.

Posibles recomendaciones adicionales de consultoría externa para tareas críticas con las que la empresa no se esté familiarizada y los recursos necesarios para el mantenimiento del sistema decantan, finalmente, a muchos gerentes a preferir pensar que un SGSI es una implantación al alcance exclusivo de unos pocos.

Hablar de “seguridad” y “gasto” es habitualmente hablar de lo mismo y la aceptación de un SGSI debe vencer al temor de la dirección a introducir desequilibrios presupuestarios por una nueva promesa de solución que no se sabe bien cuanto cuesta implantar ni como afectará a futuras partidas presupuestarias.

Para disipar estos miedos, se destacan ventajas como, precisamente, la efectividad y control de los gastos que la empresa realizará en seguridad, la mejora y adaptación continua del grado de seguridad a los cambios del entorno y la buena reputación de la empresa ligada al cumplimiento puntual de sus obligaciones legales.

Pero en términos de negocio lo que no se puede medir es como si no existiera y estas ventajas son difícilmente cuantificables. La cultura y experiencia previas en el uso de normas y sistemas de gestión o la confianza en los profesionales deben compensar, por tanto, el vacío de argumentos de negocio que serían definitivos para que las empresas desestimen las prácticas ineficientes que exponen su negocio al azar e incertidumbre.

Privacidad: Amenazas y Oportunidades		
	Amenazas	Oportunidades
Organizaciones	• Litigios • Publicidad adversa • Trastornos operacionales • Costes adicionales o inesperados • Pérdidas económicas y financieras • Fracaso de participación en los mercados	• Comunicación eficaz • Ventajas competitivas • Reducción de los costes • Identificación de nuevas necesidades • Participación inteligente en los mercados
Personas	• Spam • Discriminación • Robo de identidad • Vigilancia y control • Limitación de los derechos civiles • Subcontratación o personal temporal irregular	• Ofertas bien dirigidas • Mejora en los precios • Servicios personalizados • Atención puntual a las demandas • Establecimiento de redes de contacto fiables

En ocasiones, las obligaciones legales pueden influir en una posible reconsideración y priorizar un cambio de estrategia en esta dirección. También podríamos mencionar los incidentes graves como un mecanismo efectivo que puede inducir al cambio.

Desafortunadamente, muchos negocios no son capaces de recuperarse tras sufrir una sanción elevada o un incidente de cierta gravedad como para poder contarlo.

Dificultades tras la aceptación e implantación

Entre las empresas que determinan iniciar la implantación y certificación de un SGSI encontramos fracasos por considerar la certificación únicamente "un sello" útil y amortizable en temas de imagen y que es urgente conseguir para que el personal recupere sus actividades, tal y como eran antes de la implantación.

Por otra parte, encontramos otras empresas que logran la certificación con éxito pero que sufren dificultades a medio plazo para mantener sus SGSI por no haber localizado con antelación los recursos necesarios que garanticen estas labores básicas.

En este sentido, declaraciones como las de You Cheng Hwee, consultor especializado en seguridad y auditor principal SGSI reconocido por IRCA, confirman que,

"las compañías que desean proteger el flujo de la información interna y conseguir mayor confianza de sus socios comerciales no deberían apresurarse. El 80% de estas compañías ha fallado en la implantación de la norma ISO 27001 en seguridad."

Focalizar toda la atención y esfuerzos en las tareas propias de implantación de la norma con el propósito de que el proyecto sea lo más económico posible y lograr la certificación en un corto plazo de tiempo es un esfuerzo que deberíamos reconsiderar porque habrá que resolver todas las cuestiones que acabamos de referir.

Proponemos, por tanto, ampliar este foco de atención para considerar, adicionalmente, el análisis de importantes aspectos y procesos de negocio sobre los que un SGSI podría habilitar y potenciar estrategias con el objetivo de garantizar ventajas comerciales e incrementos notables de los beneficios a medio y largo plazo.

Presentamos un ejemplo aplicable a, prácticamente, cualquier empresa mediante el establecimiento de una relación simbiótica de la práctica de las buenas prácticas en privacidad con un SGSI.

El objetivo final que se pretende conseguir es, en todo caso, que las conclusiones sean lo suficiente sugerentes como para animar al lector a buscar y resolver nuevas fórmulas de integración de los SGSI con aquellos procesos clave de negocio que estén dentro de su propio ámbito de gestión e intereses particulares.

Gestión de la Privacidad

Según el experto consejo de Ann Cavoukian,

"No se debería proteger la privacidad por obligación, sino porque es bueno para el desarrollo del propio negocio".

Y es que la nueva economía está constituida en base a la información y, como resultado, la privacidad se ha convertido en una herramienta clave para su gestión.

La privacidad sobrepasa en influencia al factor "precio" en la sociedad de la información y es fundamental para el éxito en las relaciones de una empresa con sus clientes, con las empresas con las que colabora, con su propio personal contratado, con la sociedad en general y, en consecuencia, para lograr los objetivos propios de negocio y crecimiento.

Además de la "confidencialidad", "integridad" y "disponibilidad" ya mencionadas, podemos considerar adicionalmente la "privacidad" de la información como un elemento clave para obtener la confianza de las distintas partes interesadas en la empresa y en relación a la gestión y actividades que realiza.

La idea de considerar prácticas sólidas y demostrables de privacidad y la gestión responsable de la información sería, en definitiva, lo que hemos venido a denominar Sistema de Gestión de la Privacidad de la Información o SGPI.

Privacidad = Beneficios económicos

Las empresas que incorporan la privacidad dentro de sus valores fundamentales demuestran un alto grado de compromiso con estas prácticas y acceden, de ese modo, a nuevas oportunidades de negocio que favorecen el aumento de sus beneficios económicos.

A continuación referimos algunos ejemplos de esta relación entre privacidad y beneficios:

- Los consumidores que tienen confianza en las prácticas de privacidad de una compañía están predispuestos a incrementar su volumen de negocio (91%) y su frecuencia (90%). (Harris/Westin Poll)
- Los consumidores cesarían sus actividades (83%) con una compañía que practique abusos en el uso de su información personal. (Harris/Westin Poll)
- El 29% de los afectados por un fallo de seguridad en el que se comprometen datos personales se pasaría inmediatamente a la competencia y otro 37% consideraría esa posibilidad. Sólo un 29% esperaría a obtener antes una respuesta de la empresa. (Secure Trust Consumer Report, datos para Europa)

- El 25% de las compañías experimentó algún tipo de publicidad adversa motivada por temas de privacidad. Una de cada diez de esas compañías tuvo que enfrentarse a litigios, pérdida de oportunidades de negocio o cancelación de contratos. (Information Security Forum)
- En el 70% de las ocasiones que se piden datos personales a usuarios de la red para efectuar la compra de un producto, finalmente no se lleva a cabo por temor a que su privacidad se vea expuesta. (Narrowline Study)
- Las aprensiones de los consumidores por la ausencia de garantías en la privacidad de la Web retienen un volumen de negocio estimado en aproximadamente unos 12.000 millones de euros. (Forrester Research)
- El 73% de los consumidores evitan el uso de la banca on-line por miedo al incumplimiento en el compromiso de protección de su privacidad y más allá del robo o el hacking, incluyendo la venta de información personal para hacer negocio. (Ipsos)
- Más de un 25% de las compañías señalaron en 2004 la existencia de problemas de seguridad relacionados con los pagos como un escollo para vender por la Red. (Instituto Nacional de Estadística, España)
- En 2005 la compra online en España se incrementó un 10% respecto al año anterior debido a la mejora en la seguridad de los pagos (29,7%), una mayor variedad de productos (23,5%) y mejores precios (15%). (Asociación Española de Comercio Electrónico y Marketing Relacional).

En ocasiones se considera, únicamente, la relación que la empresa guarda con los clientes actuales pero se debería estimar, además, el importante reclamo de clientes potenciales que puede suponer la adopción de buenas prácticas en privacidad, además de la mejora en la eficacia con otras empresas y administraciones públicas.

Adicionalmente a las funciones de comunicación y transacción de la empresa hacia el exterior, es también beneficioso considerar aquellos flujos de información internos que se producen entre los diversos departamentos, filiales y sucursales.

Conclusiones finales

La información que proporciona regularmente un SGSI sobre los activos de información de la empresa permite incorporar fácilmente un proceso de estudio, identificación y consideración regular de posibles oportunidades de negocio.

Los SGSI y las buenas prácticas en privacidad habilitan a las empresas a establecer y demostrar relaciones de confianza que intensifican positivamente las actividades comerciales con sus clientes y empresas colaboradoras y facilitan su propagación a clientes potenciales.

A nivel interno, se favorece la relación que la propia empresa establece con sus empleados, la gerencia, los accionistas y otras partes interesadas y se mejora la eficacia entre distintos los ámbitos organizativos y físicos establecidos.

Un conocimiento más preciso de los niveles de satisfacción alcanzados en las actividades y procesos de negocio ayuda, además, a introducir cambios con una mayor garantía en los resultados que se desean obtener y reduce el nivel de incertidumbre y de posibles pérdidas económicas posibles en decisiones comprometidas.

Mediante la presentación del SGPI, hemos procurado cambiar la relación “seguridad-gasto” típica a una más interesante “privacidad-beneficios” y que ha sido convenientemente justificada con una serie de ejemplos significativos procedentes de algunos estudios y encuestas reconocidas en ámbitos nacionales, europeos e internacionales.

Estas consideraciones proporcionan argumentos de negocio válidos que la dirección de la empresa no puede permitirse pasar por alto y que aseguraran los recursos necesarios para proceder con la implantación y mantenimiento de un SGSI con mayores garantías de éxito.

Las empresas que consideren seriamente la privacidad dentro de sus valores principales potenciarán su negocio, explotarán al máximo su imagen y certificación en ISO 27001, adaptarán y mejorarán continuamente su nivel de protección sin tener que reducir el nivel de satisfacción de clientes o empleados, garantizarán la continuidad del negocio en cualquier situación y disfrutarán de las ventajas y herramientas esenciales para identificar y explotar puntualmente las oportunidades que los mercados ofrezcan en cada momento.

Considerando un ámbito más extenso que el de la propia empresa, debemos reseñar la positiva influencia en el entorno social que supone el desarrollo de actividades relacionadas con el tratamiento y protección de la información personal.

Sin lugar a duda, estas prácticas revalorizan las actividades de las empresas que las adoptan pero también las de los propios empleados, propagando en el entorno un valor diferenciador esencial para el desempeño de servicios profesionales que son reclamados por otras empresas cada vez con más frecuencia, así como, por cada uno de nosotros a nivel particular y en calidad de integrantes activos de esta sociedad de la información.

Otras lecturas de interés

- Relación de trabajos e informes de *Ann Cavoukian* sobre privacidad en general y prácticas sólidas de gestión responsable de la información: http://www.ipc.on.ca
- Presentaciones y lecturas de la Conferencia sobre privacidad de 2005: http://www.privacyconference2005.org/index.php?id=6#present
- "Information security management systems - Requirements", ISO/IEC 27001:2005
- Entrevista a Larry Ponemon y resultados del estudio realizado por Ponemos Institute sobre privacidad e impacto económico en las empresas: http://www.nymity.com/privaviews/2006/Ponemon.asp
- *"Una estricta política de privacidad como fuente de negocio."*: http://www.idg.es/cio/mostrarArticulo.asp?id=175292&seccion=tecnologias
- "*GTAG 5: Managing and Auditing Privacy Risks*" http://www.theiia.org
- "*Explotando un Sistema de Gestión Integrado*" por Dr. David Brewer, Dr. Michael Nash www.gammassl.co.uk http://www.iso27000.es/download/MSExploitation-SP.pdf
- "*Secure the Trust of your Brand Consumer Report*" informe del CMO Council en base a datos recogidos en EEUU, Reino Unido, Francia, Alemania, España e Italia. http://www.cmocouncil.org/General%20PDF/SecureTrustConsumerReport.pdf
- *"La ciudad de la Nueva Economía"*, conferencia de Manuel Castells. Enlace sobre el autor y otros artículos: http://weblog.educ.ar/protagonistas/archives/003477.php