Cuaderno Activa
Revista científica de la Facultad de Ingeniería

Metodología de la seguridad de la información como medida de protección en pequeñas empresas.

Methodology of Information Security as a Measure of Protection Small Business.

Giovanny Bustamante Maldonado*
Jorge Andrés Osorio Cano**

Tipo de artículo: Resultado de Investigación.

Recibido: 24 de mayo, 2014
Aceptado: 4 de agosto, 2014

Resumen

Con el auge que se vive en el uso de las tecnologías de la información y las comunicaciones (TIC), la necesidad de proteger la información manejada por estos sistemas tiene cada vez mayor importancia para las empresas. En este contexto surgen los sistemas de gestión de la seguridad de la información (SGSI), que tienen gran importancia para la estabilidad de los sistemas de información en las compañías. El hecho de poder disponer de estos sistemas es vital para la evolución de las pequeñas empresas. En este artículo se hace la caracterización de una metodología que genera conciencia sobre la importancia de la seguridad de la información y la aplicabilidad de la misma en pequeñas empresas, con lo cual se puede garantizar un tratamiento seguro de la integridad, disponibilidad y confidencialidad de la información para evitar que esta se haga pública de una manera no autorizada. La metodología recurrida se fundamenta en investigaciones relacionadas con la norma ISO 27001:2005 y su ciclo PHVA.

Palabras clave: activos, ciclo Deming (PDCA), confidencialidad, disponibilidad, integridad, ISO 27001:2005, pequeñas empresas, seguridad de la información, SGSI.

Abstract

With the boom what the information society has of Information Technology and Communications (ITC), the need to protect information is increasingly important for companies. In this context, the Systems Management Information Security (ISMS), which are of great importance for the stability of the information systems of companies arise. Being able to have these systems has become increasingly vital for the development of small businesses. This article presents a methodology that generates awareness of the importance of information security, and the applicability of it in small businesses, ensuring a safe treatment for the integrity, availability and confidentiality, to avoid characterized such information becomes public in an unauthorized manner. The methodology used is based on research related to the topic of ISO 27001: 2005 and PDCA cycle.

Keywords: assets Deming cycle (PDCA), confidentiality, availability, integrity, ISO 27001: 2005, small business, information security, ISMS.

* Licenciado en docencia de computadores. Esp. Seguridad de la Información. Gerente, Help Desk System. giovybm@yahoo.es

** Licenciado en docencia de computadores. Esp. Seguridad de la Información. Universidad de Medellín. andreso78@hotmail.com

Introducción

La seguridad de la información, según la norma ISO 27001:2005, "consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización". Igualmente, se puede complementar con la definición del Ingeniero y Magister en Sistemas Jeimy Cano: "La Seguridad de la Información es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información" (Cano, 2011). Si se buscaran más definiciones, seguramente se encontrarían enormes cantidades de ellas que circundan la misma idea.

Con relación a lo anterior, la Asociación Española de Normalización y Certificación (AENOR, 2010) afirma que "la información es uno de los principales activos de las organizaciones. La defensa de este activo es una tarea esencial para asegurar la continuidad y el desarrollo del negocio, así como también es una exigencia legal (protección de la propiedad intelectual, protección de datos personales, servicios para la sociedad de la información), y además traslada confianza a los clientes y/o usuarios. Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada.

Los Sistemas de Gestión de Seguridad de la Información (SGSI) son el medio más eficaz de minimizar los riesgos, al asegurar que se identifican y valoran los activos y sus riesgos, considerando el impacto para la organización, y se adoptan los controles y procedimientos más eficaces y coherentes con la estrategia de negocio".

Los SGSI constituyen el concepto central sobre el que se construye la norma ISO/IEC 27001, la cual especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI. Esta norma es la principal de la serie ISO 27000, publicada en su primera edición en el año 2005, adoptando el ciclo de Deming como metodología que puede ser aplicada a todos los procesos que abarca un SGSI (ISO27000.es, 2005). Esta metodología es mejor conocida por su sigla en inglés, PDCA: Plan (planear) – Do (hacer) – Check (verificar) – Act (actuar).

Este artículo se desarrolla de la siguiente forma: en la sección 2 se presenta la metodología, en la sección 3 se fundamenta el marco general para contextualizar la importancia de caracterizar la metodología de un SGSI en una pequeña empresa, luego en la sección 4 se describe el conjunto de pasos que se debe tener en cuenta para que las pequeñas empresas caractericen su metodología a través del ciclo Deming, y por último, en la sección 5 se presentan las conclusiones.

Metodología

En el presente artículo se establece el análisis de un sistema de gestión de seguridad de la información (SGSI) en pequeñas empresas del sector tecnológico, a partir de la caracterización del ciclo Deming, con el fin de que sea utilizado en estas unidades de negocios.

Marco general

Se considera que las pequeñas empresas, por lo general, no acogen un SGSI debido a que muchas se concentran en la realización de sus productos, por lo que no contemplan la información y su seguridad como un todo ni como un ítem relevante; otras no cuentan con recursos que financien los montos necesarios para implementar la seguridad de la información. Es por ello que se pretende caracterizar una metodología accesible de seguridad de la información como medida de protección en pequeñas empresas.

Se ha escrito poco sobre la seguridad de la información y su papel desempeñado dentro

de las pequeñas empresas; por eso, este marco pretende expresar aportes que han enriquecido los estándares de prácticas de seguridad de la información, y desde la perspectiva de los autores, diseñar un posible direccionamiento de la norma (ISO 27001, 2005).

A continuación se presentan algunas definiciones importantes relacionadas al SGSI que se busca diseñar:

Activo: Cualquier elemento o información, tenga o no valor contable para la organización (ISO 13335-1, 2004).

Amenaza: Causa potencial de un incidente no deseado, que podría dañar uno o más activos de un sistema u organización (ISO 27000, 2014).

Control: Los medios de gestión de riesgos, incluidas las políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o naturaleza jurídica (ISO 27002, 2005).

Información: Está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente (Definición. DE, 2008).

Pequeña empresa: Es considerada como tal si en ella trabajan entre 6 y 50 personas. Suele tener varios ramos de actividad y más de un establecimiento de comercio o lugar de trabajo. Normalmente, necesita financiación a través de líneas de crédito y presentar información a sus acreedores o prestamistas. Su nómina puede ser extensa y relativamente compleja, requiere de información sobre la gestión de su negocio, además de costos analizados por ramos o líneas de producción (Agudelo, 2002).

Para el Ministerio de Comercio, Industria y Turismo de Colombia, los parámetros vigentes para clasificar las pequeñas empresas son los siguientes (MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO - MINCIT, 2013):

- Planta de personal entre once (11) y cincuenta (50) trabajadores.

- Activos totales por valor entre quinientos uno (501) y menos de cinco mil (5.000) salarios mínimos mensuales legales vigentes.

Riesgo: Combinación de la probabilidad de materialización de una amenaza y el daño que produciría sobre un activo (ISO 13335-1, 2004).

Seguridad: Es un concepto asociado a la certeza, falta de riesgo o contingencia. Podemos entender como seguridad un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen (AEC, 2013). Se toman como referencia dos tipos:

- *Seguridad física:* Implica el empleo de las personas, la tecnología y los materiales para proteger una instalación, campus, infraestructura crítica o zona de alto valor contra los efectos del acceso no autorizado, robo, incendio, destrucción maliciosa, terrorismo, pérdida u otro delito intencional o daño. NIST tiene varios proyectos y programas que trabajan en esta área (NIST, 2012).

- *Seguridad lógica:* Consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solamente permita acceder a ellos a las personas autorizadas para hacerlo (Borghello, 2009).

Seguridad de la información: Protección de la información y de los accesos a los sistemas de información, control de su uso, divulgación, alteración, modificación, lectura, registro o destrucción.
La norma (ISO 27001, 2005) ayudará a proteger la información en términos de:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados (ISO 27000, 2014).
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso (ISO 27000, 2014).
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran (ISO 27000, 2014).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una amenaza (ISO 27000, 2014).

Con el transcurrir del tiempo, la seguridad de la información ha tomado mayor importancia, atrayendo consigo a un grupo de especialistas en temas relacionados con seguridad, riesgos y afines, quienes desarrollan diversos marcos de trabajo, metodologías, estándares, buenas prácticas y distintos modelos para diseñar un SGSI, leyes, normativas, entre otros, con el fin de brindar a las empresas la oportunidad de adoptarlas y proteger adecuadamente su información.

Norma ISO/IEC 27001:2005

Como señala la 27001 Academy, la ISO/IEC 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La primera revisión se publicó en 2005 y fue desarrollada con base en la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información dentro de una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización, en cumplimiento con la norma ISO 27001.

Metodología ciclo Deming

El propósito de un SGSI no es garantizar la seguridad -que nunca podrá ser resuelta en un 100%- sino garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la pequeña empresa de una forma documentada, sistemática, estructurada, continua, repetible, eficiente y adaptada a los cambios que se produzcan en la organización, los riesgos, el entorno y las tecnologías.

Un SGSI ayuda a establecer estas políticas y procedimientos en relación con los objetivos de negocio de la pequeña empresa, con el objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, una pequeña empresa conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una política definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Ciclo Deming o PDCA

Comprende, como principal objetivo, caracterizar una metodología que genere conciencia sobre la importancia de la seguridad de la información y la aplicabilidad de la misma en pequeñas empresas, que garantice un tratamiento seguro de la integridad, disponibilidad y confidencialidad para evitar que dicha información se vuelva pública de una manera no autorizada.

La norma ISO 27001 adopta el ciclo de Deming como metodología, la cual se puede aplicar a todos los procesos que abarca el SGSI. Esta metodología es conocida por sus siglas en inglés PDCA: Plan-Do- Check-Act (Aliaga, 2013).

El ciclo PDCA (o PHVA en español) es una herramienta para la mejora continua, diseñada por el Dr. Walter Shewhart en el año 1920 y presentada por Edwards Deming a partir del año 1950, la cual se basa en un ciclo de cuatro pasos (Díaz, 2010). Plan (planificar), Do (hacer), Check (verificar) y Act (actuar). A continuación, se describirán brevemente los pasos que se siguen en el ciclo de Deming (Aliaga, 2013). Plan (planificar): Se establecen las actividades y procesos necesarios para alcanzar los resultados esperados establecidos por la(s) parte(s) interesada(s).

Do (hacer): Se implementa el plan establecido, se ejecutan los procesos estudiados y, finalmente, se empieza a desarrollar el producto. Check (verificar): Se estudian los resultados luego de ejecutar los procesos y actividades mencionados en el "Do" y los compara con los resultados esperados del "Plan" para analizar posibles diferencias.

Act (actuar): Se realizan acciones correctivas para alcanzar los resultados esperados, si es que hubiera alguna diferencia con los resultados obtenidos.

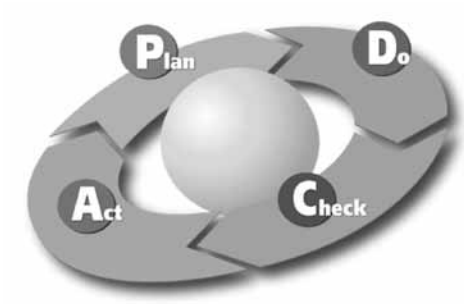


Figura 1. Fases del ciclo PDCA
Fuente: Bulsuk (2009)

La gestión de la seguridad de la información -como casi cualquier proceso de gestión- tiene tres pilares que deben ser tenidos en cuenta, los cuales interactúan mutuamente: personas, procesos y tecnología.

Por lo tanto, el SGSI deberá considerar el contexto de la pequeña empresa y sus características culturales. Deberá, además, ser sostenible en el tiempo, con capacidad de incorporar mejoras de forma incremental y continua, con un beneficio comprobable para la organización.

Para ello se requiere de una metodología bien definida, que acompañe el dinamismo necesario de la pequeña empresa o de cualquier organización, y a su vez respete las estrategias empresariales y su vinculación estructural. La Tabla 1 caracteriza los procesos establecidos por el ciclo PDCA en cuanto a diseño y monitoreo de un SGSI.

Tabla 1. Procesos desarrollados por el ciclo PDCA

CICLO PDCA	PROCESOS
Plan (planificar) Establecer el SGSI	Establecer la política, objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Do (hacer) Implementar y operar el SGSI	Implementar y operar la política, los controles, procesos y procedimientos del SGSI.
Check (verificar) Hacer seguimiento y revisar el SGSI	Evaluar y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección para su revisión.
Act (actuar) Mantener y mejorar el SGSI	Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

Fuente: ISO 27001 (2005)

Resultados

En este artículo se caracterizó la metodología del ciclo PDCA -fuertemente recomendada por la Organización Internacional de Normalización (ISO)- que ayuda alcanzar los objetivos y a conseguir los resultados esperados de una empresa. Esta metodología es la más usada para este tipo de proyectos porque analiza aspectos como: las políticas de seguridad de la información, la organización para la seguridad de la información, la clasificación y control de activos informáticos, las políticas del personal respecto a la seguridad informática, la seguridad física y ambiental de los sistemas de información, la gestión de las comunicaciones de datos y operaciones de los sistemas informáticos, el control de acceso a los sistemas informáticos, el desarrollo y mantenimiento de sistemas informáticos, la gestión de incidentes de sistemas informáticos, la administración de la continuidad de los sistemas informáticos y el cumplimiento legal referido a los sistemas informáticos.

Conclusiones

Al hablar de la seguridad de la información, que tiene como fin la protección de la misma y con especial énfasis en la pequeña empresa, se debe tener en cuenta que la seguridad absoluta no es posible; no existe un sistema 100% seguro, de forma que el elemento de riesgo estará siempre presente, independiente de las medidas que se tomen, las cuales deben ser fruto de un proceso sistemático, documentado y conocido por la pequeña empresa. Este proceso constituye un sistema de gestión de seguridad de la información (SGSI), cuyo diseño y caracterización está influenciado por las necesidades y objetivos, requerimientos de seguridad, procesos empleados y el tamaño y estructura de la organización. Para ello el contenido de la norma ISO 27001 está orientado al tratamiento del SGSI mediante la gestión de riesgos, ya que describe la forma de mantener y mejorar la seguridad de los activos de información en cualquier organización, y que puede ser utilizada junto con la metodología del ciclo Deming.

La metodología ciclo Deming o PDCA, en un sistema de gestión de seguridad de la información (SGSI), permite descubrir los puntos vulnerables de una organización y provee herramientas valiosas para diseñar procesos y procedimientos de seguridad eficaces. Esta metodología garantiza confidencialidad, integridad y disponibilidad de los activos de un negocio.

Las pequeñas empresas, al contrario de las grandes organizaciones, carecen de recursos humanos, técnicos y económicos para afrontar el mantenimiento de la seguridad en sus sistemas de información, por lo tanto necesitan una herramienta sencilla y de bajo costo que dé respuesta a los riesgos existentes. La adopción de un SGSI es una alternativa adecuada para que la empresa establezca una serie de medidas para ordenar, sintetizar y simplificar de manera continua el esfuerzo que ya se hace -o que ya se debería hacer- en seguridad de la información.

Referencias

AEC. (2013). *Asociación Española para la Calidad (AEC)*. Recuperado de http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion.

AENOR. (2010). AENOR. Recuperado de https://www.aenor.es/AENOR/certificacion/seguridad/seguridad_27001.asp#.VEW_N_l5Ob8

Agudelo, F. T. (2002). *Pequeñas y medianas empresas: generalidades*. Recuperado de http://www.javeriana.edu.co/fcea/cuadernos_contab/vol3_n_14/vol3_14_1.pdf

Aliaga, L. C. (2013). *Diseño de un sistema de gestión de seguridad de información para un instituto educativo*. Tesis para optar por el Título de Ingeniero Informático, Pontificia Universidad Católica del Perú, Lima.

Borghello, C. (2009). *Segu.info seguridad de la información*. Recuperado de http://www.segu-info.com.ar/logica/seguridadlogica.htm

Bulsuk, K. G. (2009). *Karngbulsuk*. Recuperado de http://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html

Cano, J. J. (2011). *ISACA*. Recuperado de http://www.isaca.org/Journal/Past-Issues/2011/Volume-5/Pages/JOnline-La-Gerencia-de-la-Seguridad-de-la-Informacion-Evolucion-y-Retos-Emergentes.aspx

Definición. DE. (2014). *Definición*. Disponible en: http://definicion.de

Diaz, J. (2010). Negocios y emprendimiento. Recuperado de http://www.negociosyemprendimiento.org/2010/08/plantilla-para-aplicar-el-ciclo-phva-de.html

INCIBE. (2009). *Instituto Nacional de Ciberseguridad*. Recuperado de https://www.incibe.es/pressRoom/Prensa/Actualidad_INCIBE/diplomas_SGSI_pymes/?year=2009

ISO 13335-1. (2004). ISO/IEC 13335-1:2004 *Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management*. Recuperado de http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066

ISO 27000. (2014). ISO/IEC 27000:2014 Information technology - Security techniques - Information security management systems - Overview and vocabulary. Recuperado de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=63411

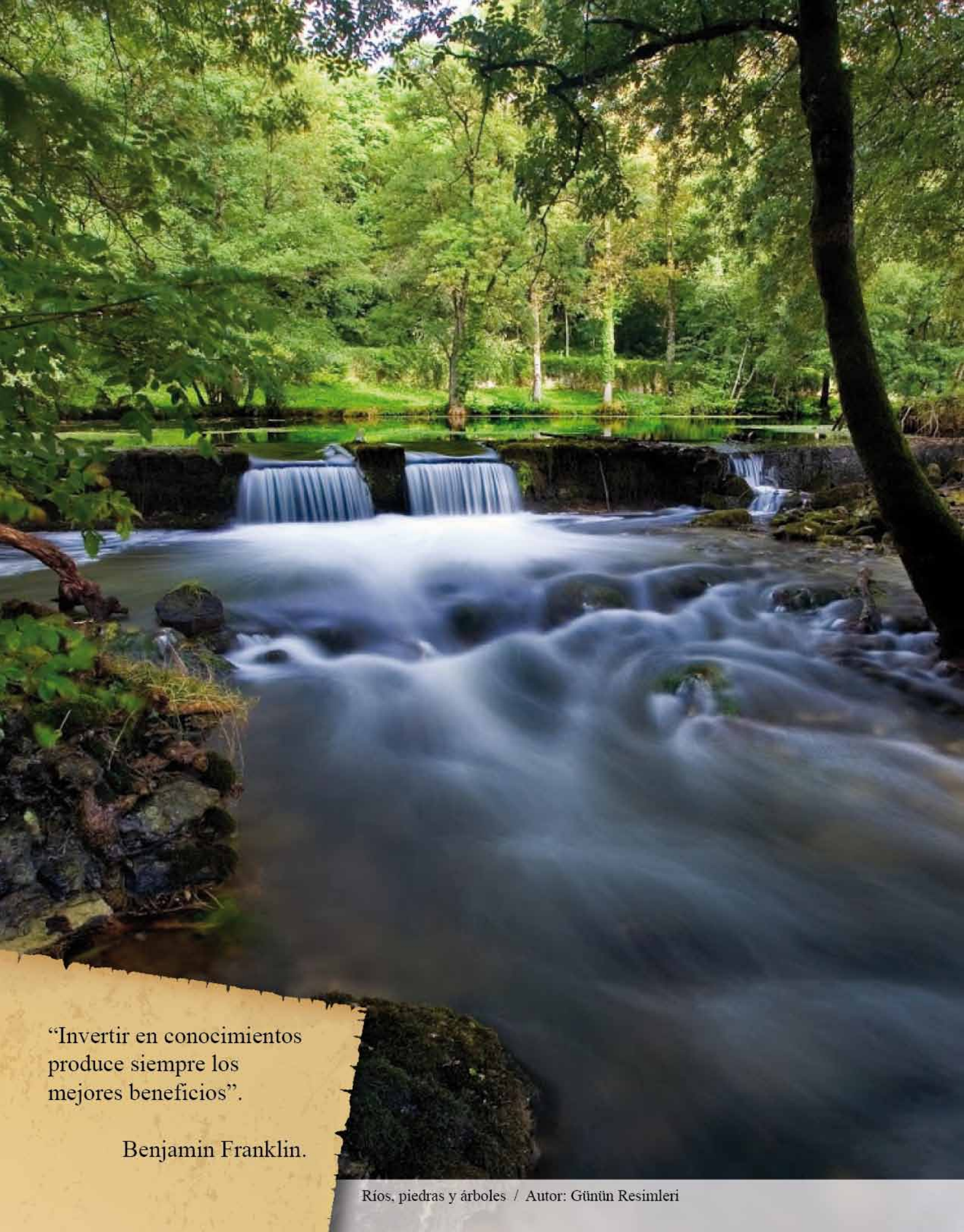
ISO 27000 (2005). El portal de ISO 27001 en español. Recuperado de http://www.iso27000.es/sgsi.html

ISO27001. (2005). ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Requirements. Recuperado de http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

ISO 27002 (2005). ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management. Recuperado de http://www.iso.org/iso/catalogue_detail?csnumber=50297

Ministerio de Comercio, Industria y Turismo - MINCIT. (2013). Parámetros vigentes. Recuperado de http://www.mipymes.gov.co/publicaciones.php?id=2761

NIST. (2012). The National Institute of Standards and Technology (NIST) is an agency of the U.S. Recuperado de http://www.nist.gov/oles/physicalsecurity.cfm



"Invertir en conocimientos produce siempre los mejores beneficios".

Benjamin Franklin.

Ríos, piedras y árboles / Autor: Günün Resimleri