DIRECTRICES PARA LA DEFINICIÓN E IMPLANTACIÓN DE POLÍTICAS DE SEGURIDAD

Álvaro Gómez Vieites
agomezvieites@gmail.com
Profesor de la Escuela de Negocios Caixanova

RESUMEN DE LA PONENCIA

En esta ponencia se presentan los conceptos básicos sobre Políticas, Planes y Procedimientos de seguridad, presentando la jerarquía de elementos a considerar, comenzando por los objetivos fundamentales de la Gestión de la Seguridad de la Información, resumidos mediante el acrónimo CIA (Confidencialidad, Integridad y Disponibilidad de la información).

Seguidamente, se estudian cuáles son las principales características y requisitos que deberían cumplir las Políticas de Seguridad, y se analizan las principales dificultades a tener en consideración a la hora de definir las Políticas de Seguridad

A continuación se describen todos los aspectos que es necesario considerar para poder definir e implantar las Políticas de Seguridad: alcance; objetivos; compromiso de la Dirección; inventario de recursos; análisis y gestión de riesgos; asignación de responsabilidades; comportamientos exigidos y prohibidos del personal; identificación de las medidas, normas y procedimientos de seguridad a implantar; relaciones con terceros; gestión de incidentes; planes de contingencia y de continuidad del negocio; etc.

Asimismo, también se analiza el papel de los distintos colectivos que deberían estar implicados en la definición de las Políticas de Seguridad dentro de una organización.

Por último, la ponencia incluye una serie de consejos y pautas para facilitar la implantación y actualización de las Políticas de Seguridad.

1. CONCEPTOS BÁSICOS

Podemos definir una **Política de Seguridad** como una "declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran" (RFCs 1244 y 2196).

Un **Plan de Seguridad** es un conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos.

Por último, un **Procedimiento de Seguridad** es la definición detallada de los pasos a ejecutar para llevar a cabo unas tareas determinadas. Los Procedimientos de Seguridad permiten aplicar e implantar las Políticas de Seguridad que han sido aprobadas por la organización.

En la siguiente figura se representa la jerarquía de conceptos manejados al hablar de las Políticas, Planes y Procedimientos de Seguridad:

Figura 1: Políticas, Planes y Procedimientos de Seguridad

Así, en la cúspide de la pirámide se situarían los objetivos fundamentales de la Gestión de la Seguridad de la Información, resumidos mediante el acrónimo CIA (Confidencialidad, Integridad y Disponibilidad de la información). Una vez fijados los objetivos fundamentales, es necesario definir las Políticas de Seguridad, así como los Planes y Procedimientos de actuación para conseguir su implantación en la organización.

Los Procedimientos de Seguridad se descomponen en tareas y operaciones concretas, las cuales, a su vez, pueden generar una serie de registros y evidencias que facilitan el

seguimiento, control y supervisión del funcionamiento Sistema de Gestión de la Seguridad de la Información.

Los Procedimientos de Seguridad permiten implementar las Políticas de Seguridad definidas, describiendo cuáles son las actividades que se tienen que realizar en el sistema, en qué momento o lugar, quiénes serían los responsables de su ejecución y cuáles serían los controles aplicables para supervisar su correcta ejecución.

En este sentido, las Políticas definen **qué** se debe proteger en el sistema, mientras que los Procedimientos de Seguridad describen **cómo** se debe conseguir dicha protección. En definitiva, si comparamos las Políticas de Seguridad con las Leyes en un Estado de Derecho, los Procedimientos serían el equivalente a los Reglamentos aprobados para desarrollar y poder aplicar las Leyes.

Así, a modo de ejemplo, podríamos citar como procedimientos la planificación de las tareas administrativas y de sus responsables: administración de las cuentas de usuario y de los controles de acceso a los recursos lógicos; realización y supervisión de las copias de seguridad; seguimiento de los eventos de seguridad; etcétera. Otro grupo de procedimientos de seguridad estaría relacionado con la instalación, configuración y mantenimiento de distintos elementos de seguridad: cortafuegos (firewalls), servidores proxy, antivirus, Sistemas de Detección de Intrusiones (IDS)…

En la siguiente tabla se presenta otro ejemplo de la relación entre una determinada directriz o Política de Seguridad, los procedimientos que de ella se derivan y las tareas concretas que debería realizar el personal de la organización.

Política	Procedimiento	Tareas a realizar
Protección del servidor Web de la organización contra accesos no autorizados	Actualización del software del servidor Web	✓Revisión diaria de los parches publicados por el fabricante ✓Seguimiento de las noticias sobre posibles fallos de seguridad
	Revisión de los registros de actividad en el servidor	✓Revisión semanal de los "*logs*" del servidor para detectar situaciones anómalas ✓Configuración de alertas de seguridad que permitan reaccionar de forma urgente ante determinados tipos de ataques e intentos de intrusión

Figura 2: Ejemplo de Política y Procedimientos de Seguridad

2. CARACTERÍSTICAS DESEABLES DE LAS POLÍTICAS DE SEGURIDAD

En este apartado se presentan de forma esquemática las principales características y requisitos que debería cumplir las Políticas de Seguridad:

- Las Políticas de Seguridad deberían poder ser implementadas a través de determinados procedimientos administrativos y la publicación de unas guías de uso aceptable del sistema por parte del personal, así como mediante la instalación, configuración y mantenimiento de determinados dispositivos y herramientas hardware y software que implanten servicios de seguridad.
- Deben definir claramente las responsabilidades exigidas al personal con acceso al sistema: técnicos, analistas y programadores, usuarios finales, directivos, personal externo a la organización...
- Deben cumplir con las exigencias del entorno legal (Protección de Datos Personales –LOPD–, Protección de la Propiedad Intelectual, Código Penal...).
- Se tienen que revisar de forma periódica para poder adaptarlas a las nuevas exigencias de la organización y del entorno tecnológico y legal. En este sentido, se debería contemplar un procedimiento para garantizar la revisión y actualización periódica de las Políticas de Seguridad.
- Aplicación del principio de "Defensa en Profundidad": definición e implantación de varios niveles o capas de seguridad. Así, si un nivel falla, los restantes todavía podrían preservar la seguridad de los recursos del sistema. De acuerdo con este principio, es necesario considerar una adecuada selección de medidas de prevención, de detección y de corrección.
- Asignación de los mínimos privilegios: los servicios, aplicaciones y usuarios del sistema deberían tener asignados los mínimos privilegios necesarios para que puedan realizar sus tares. La política por defecto debe ser aquella en la que todo lo que no se encuentre expresamente permitido en el sistema estará prohibido. Las aplicaciones y servicios que no sean estrictamente necesarios deberían ser eliminados de los sistemas informáticos.
- Configuración robusta ante fallos: los sistemas deberían ser diseñados e

implementados para que, en caso de fallo, se situaran en un estado seguro y cerrado, en lugar de en uno abierto y expuesto a accesos no autorizados.

- Las Políticas de Seguridad no deben limitarse a cumplir con los requisitos impuestos por el entorno legal o las exigencias de terceros (clientes, Administración Pública…), sino que deberían estar adaptadas a las necesidades reales de cada organización.

3. DIFICULTADES AL DEFINIR LAS POLÍTICAS DE SEGURIDAD

La organización también debería tener en consideración cuáles son las principales dificultades a la hora de definir las Políticas de Seguridad.

Así, en primer lugar conviene destacar que la información constituye un recurso que en muchos casos no se valora adecuadamente por su intangibilidad, situación que no se produce con los equipos informáticos, la documentación o las aplicaciones informáticas.

Además, con la proliferación de las redes de ordenadores, la información de las empresas ha pasado de concentrarse en los grandes sistemas (sistemas centralizados) a distribuirse por los ordenadores y servidores ubicados en los distintos departamentos y grupos de trabajo. Por este motivo, en la actualidad muchas organizaciones no conocen con precisión toda la información que hay en los puestos de trabajo (generalmente, ordenadores personales de la propia organización), ni los riesgos que tienen de sufrir ataques u otro tipo de desastres, ni cómo la propia organización utiliza esa información.

Debemos tener en cuenta dos aspectos contradictorios en las redes y sistemas informáticos: por un lado, su principal razón de ser es facilitar la comunicación y el acceso a la información y, por otro, asegurar que sólo acceden a ella los usuarios debidamente autorizados. Esta contradicción está presente continuamente, ya que las medidas adoptadas para mejorar la seguridad (autenticación, control de los accesos, monitorización del uso, cifrado, herramientas de detección de ataques, antivirus...) dificultan el uso de las redes y sistemas, al ralentizar los accesos e imponer ciertas restricciones, por lo que es necesario mantener un compromiso entre la usabilidad y rendimiento de los sistemas informáticos, por un parte, y su seguridad, por otra.

Otro factor importante, que muchas veces se olvida, es que, según numerosos estudios publicados, más del 75% de los problemas inherentes a la seguridad se producen por fallos de los equipos o por un mal uso por parte del personal de la propia organización. Por este motivo, las Políticas de Seguridad deben contemplar no sólo los ataques provenientes del mundo exterior ajeno a la organización, sino también los procedimientos de uso interno, prestando especial atención a la formación y sensibilización de los empleados y directivos.

La adopción de determinadas medidas burocráticas (registro de entradas y salidas, inventario de soportes informáticos…) o de determinados controles y procedimientos de seguridad se traducen generalmente en una mayor incomodidad para los usuarios, por lo que resultará fundamental explicar la importancia de la correcta aplicación de estas medidas para mejorar la seguridad en el trabajo cotidiano con los recursos de la organización.

Los problemas con las aplicaciones y programas informáticos (productos incompletos o defectuosos que requieren de la aplicación de continuos parches y actualizaciones de seguridad), los continuos cambios en el entorno tecnológico y normativo, la creciente complejidad de los sistemas informáticos, así como la cada vez mayor dependencia de las conexiones a Internet y de los accesos y servicios remotos son factores que han venido a complicar aún más, si cabe, el escenario en el que tienen que definirse e implantarse las medidas de seguridad.

Además, las medidas de seguridad no contribuyen a mejorar la productividad de los sistemas y redes informáticas, sino, más bien, todo lo contrario, ya que pueden reducir el rendimiento de los equipos y las aplicaciones (los sistemas criptográficos, por ejemplo, consumen mayores recursos computacionales y ancho de banda en las conexiones a Internet), por lo que las organizaciones son reticentes a dedicar recursos a esta tarea.

Sin embargo, es necesario contar con los adecuados recursos técnicos, humanos y organizativos, así como de una dotación presupuestaria suficiente para conseguir una adecuada implantación de las Políticas de Seguridad definidas por la organización. No invertir en seguridad informática en una organización del siglo XXI sería como circular en un automóvil sin seguro frente a terceros: en caso de accidente las consecuencias pueden ser muy graves para el propietario y los acompañantes.

No se debe olvidar que la finalidad última del Departamento de Informática es

proporcionar las herramientas y la información que van a necesitar los usuarios para poder llevar a cabo su trabajo de forma sencilla y eficiente (y, por supuesto, de forma segura). Sin embargo, en muchas organizaciones se sacrifica la seguridad por la usabilidad y rendimiento del sistema, primando de este modo la productividad.

4. DEFINICIÓN E IMPLANTACIÓN DE LAS POLÍTICAS DE SEGURIDAD

A la hora de definir las Políticas de Seguridad en una organización, sería conveniente contemplar todos los aspectos que se enumeran a continuación:

- Alcance: recursos, instalaciones y procesos de la organización sobre los que se aplican.
- Objetivos perseguidos y prioridades de seguridad.
- Compromiso de la Dirección de la organización.
- Clasificación de la información e identificación de los activos a proteger.
- Análisis y gestión de riesgos.
- Elementos y agentes involucrados en la implantación de las medidas de seguridad.
- Asignación de responsabilidades en los distintos niveles organizativos.
- Definición clara y precisa de los comportamientos exigidos y de los que están prohibidos ("*Appropriate Use Policy*") por parte del personal.
- Identificación de las medidas, normas y procedimientos de seguridad a implantar.
- Gestión de las relaciones con terceros (clientes, proveedores, partners...).
- Gestión de incidentes.
- Planes de contingencia y de continuidad del negocio.
- Cumplimiento de la legislación vigente.
- Definición de las posibles violaciones y de las consecuencias derivadas del incumplimiento de las Políticas de Seguridad.

Además, la organización debería contemplar la seguridad en todas las fases del Ciclo de Vida de los Sistemas Informáticos. En las Políticas de Seguridad se deberían definir cuáles son estas medidas de seguridad relacionadas con el desarrollo, implantación y mantenimiento de las aplicaciones informáticas, estableciendo una clara separación entre los entornos de desarrollo y los sistemas en producción. Todos los cambios y actualizaciones realizados en las aplicaciones deberían ser probados de forma segura y en un entorno independiente, antes de su puesta en marcha como un sistema en producción.

Las Políticas de Seguridad también deberían reflejar los requisitos de seguridad aplicables a todas las operaciones relacionadas con la administración y mantenimiento de la red y de los equipos informáticos. Asimismo, será necesario especificar el personal implicado en cada tipo operación, así como los procedimientos que se deberían seguir para respetar los requisitos mínimos de seguridad.

Las Políticas de Seguridad relacionadas con la subcontratación de determinados trabajos y actividades a proveedores externos requieren contemplar aspectos tales como la negociación de los mínimos niveles de servicio y calidad, en especial con aquellos proveedores relacionados con la informática, las comunicaciones o el tratamiento de los datos.

Asimismo, se debería exigir el cumplimiento de ciertas medidas de seguridad que puedan afectar al sistema informático de la organización. Este aspecto resulta de especial importancia en los tratamientos de datos personales, ya que así lo exigen leyes como la Ley Orgánica de Protección de Datos en España.

En la Política de Relación con Proveedores se deberían estipular las cláusulas y exigencias habituales en la firma de contratos con los proveedores, a fin de delimitar las responsabilidades y los requisitos del servicio contratado.

5. COLECTIVOS IMPLICADOS Y SEGURIDAD FRENTE AL PERSONAL

Podemos señalar cuáles son los distintos colectivos que deberían estar implicados en la definición de las Políticas de Seguridad dentro de una organización:

- Directivos y responsables de los distintos departamentos y áreas funcionales de la organización.
- Personal del Departamento de Informática y de Comunicaciones.

- Miembros del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT, *Computer Security Incident Response Team*), en caso de que éste exista.
- Representantes de los usuarios que pueden verse afectados por las medidas adoptadas.
- Consultores externos expertos en seguridad informática.

La organización debe definir con claridad cuáles son los distintos niveles de acceso a los servicios y recursos de su sistema informático.

De este modo, en función de las distintas atribuciones de los usuarios y del personal de la organización, se tendrá que establecer quién está autorizado para realizar una serie de actividades y operaciones dentro del sistema informático; a qué datos, aplicaciones y servicios puede acceder cada usuario; desde qué equipos o instalaciones podrá acceder al sistema y en qué intervalo temporal (día de la semana y horario).

En relación con este aspecto de la seguridad, la organización debe prestar especial atención a la creación de cuentas de usuarios y la asignación de permisos de acceso para personal ajeno a ésta, que pueda estar desempeñando con carácter excepcional determinados trabajos o actividades que requieran de su acceso a algunos recursos del sistema informático de la organización.

Asimismo, será necesario establecer qué datos y documentos podrá poseer o gestionar cada empleado.

Sería conveniente aplicar el principio de segregación de responsabilidades, en virtud del cual determinados privilegios no podrán ser ostentados por la misma persona dentro del sistema informático de la organización.

La organización deberá informar puntualmente a sus empleados con acceso al sistema de información de cuáles son sus obligaciones en materia de seguridad. Asimismo, debería llevar a cabo acciones de formación de manera periódica para mejorar los conocimientos informáticos y en materia de seguridad de estos empleados.

Del mismo modo, las personas que se incorporen a la organización tendrán que ser informadas y entrenadas de forma adecuada, sobre todo en las áreas de trabajo con acceso a datos sensibles y aplicaciones importantes para el funcionamiento de la organización.

Por otra parte, la organización también debe contemplar la privacidad de los usuarios que tienen acceso a estos recursos y servicios del sistema informático, estableciendo en qué condiciones sus ficheros, mensajes de correo u otros documentos podrían ser intervenidos por la organización.

Todas estas medidas deberían completarse con la preparación de una serie de manuales de normas y procedimientos, que incluyesen las medidas de carácter administrativo y organizativo adoptadas para garantizar la adecuada utilización de los recursos informáticos por parte del personal de la organización.

Asimismo, será necesario definir cuáles son las posibles violaciones de las Políticas de Seguridad, de sus consecuencias para los responsables y de las medidas y pasos a seguir en cada caso.

También sería aconsejable una revisión de las medidas y directrices definidas en las Políticas de Seguridad por parte de los asesores legales de la organización.

6. OTROS CONSEJOS PARA FACILITAR LA IMPLANTACIÓN DE LAS POLÍTICAS DE SEGURIDAD

De cara a facilitar su difusión en el seno de la organización, resultará fundamental poner en conocimiento de todos los empleados que se puedan ver afectados por las Políticas de Seguridad cuáles son los planes, normas y procedimientos adoptados por la organización.

El establecimiento claro y preciso de cuáles son las actuaciones exigidas, las recomendadas y las totalmente prohibidas dentro del sistema informático o en el acceso a los distintos recursos e información de la organización, citando ejemplos concretos que faciliten su comprensión por parte de todos los empleados, contribuirán a la difusión e implantación de estas medidas.

Asimismo, el acceso a documentación clara y detallada sobre todas las medidas y directrices de seguridad, así como los planes de formación y sensibilización inicial de los nuevos empleados que se incorporan a la organización son otros dos aspectos de vital importancia. La documentación debería incluir contenidos sencillos y asequibles para personal no técnico, incorporando un glosario con la terminología técnica empleada en los distintos apartados. En todo momento, los autores deberían ponerse en el lugar del lector a la hora de preparar los materiales para dar a conocer las Políticas de Seguridad.

En cada documento se podría incluir la siguiente información:

- Título y codificación.
- Fecha de publicación.
- Fecha de entrada en vigor.
- Fecha prevista de revisión o renovación.
- Ámbito de aplicación (a toda la organización o sólo a un determinado departamento o unidad de negocio).
- Descripción detallada (redactada en términos claros y fácilmente comprensibles por todos los empleados) de los objetivos de seguridad.
- Persona responsable de la revisión y aprobación.
- Documento (o documentos) al que reemplaza o modifica.
- Otros documentos relacionados.

En los procedimientos de seguridad será necesario especificar además otra información adicional:

- Descripción detallada de las actividades que se deben ejecutar.
- Personas o departamentos responsables de su ejecución.
- Momento y/o lugar en que deben realizarse.
- Controles para verificar su correcta ejecución.

La implantación de un adecuado sistema de gestión documental facilitará el registro, clasificación y localización de toda la documentación que se haya generado, además de constituir un aspecto fundamental si la organización desea conseguir la certificación del Sistema de Gestión de Seguridad de la Información.

Por otra parte, la organización debería tener identificado al personal clave para garantizar el adecuado nivel de cumplimiento de las normas y procedimientos de seguridad. En estos casos, se podría solicitar la firma de una carta o documento por parte de estos empleados en el que se comprometan a cumplir con las directrices y principios establecidos en las Políticas de Seguridad de la organización. También se podrían contemplar las obligaciones y responsabilidades mediante una serie de cláusulas anexas al contrato laboral de cada uno de estos empleados. Esta medida podría extenderse, si se considera necesario, a todo el personal de la organización.

Las Políticas de Seguridad constituyen una herramienta para poder hacer frente a futuros problemas, fallos de sistemas, imprevistos o posibles ataques informática. Sin embargo, se puede incurrir en una falsa sensación de seguridad si las Políticas de Seguridad no se han implantado correctamente en toda la organización.

En consecuencia, la organización debería tratar de evitar que las Políticas de Seguridad se conviertan en un libro más en las estanterías de sus despachos. En este sentido, para conseguir una implantación real y eficaz de las medidas y directrices definidas será necesario contar con el compromiso e implicación real de los directivos de la organización, aspecto fundamental para poder disponer de los recursos necesarios y para que su actuación sirva de guía y referencia para el resto de los empleados.

Asimismo, se podrían adoptar una serie de medidas para recordar la importancia de la seguridad a los distintos empleados de la organización en el día a día: mostrar mensajes de aviso al entrar en el sistema; utilizar diverso material impreso (alfombrillas, carteles informativos, etcétera) para recordar las principales directrices de seguridad; llevar a cabo sesiones periódicas de formación y sensibilización de los empleados...

Por otra parte, la organización también debe contemplar una serie de actuaciones para verificar el adecuado nivel de cumplimiento e implantación de las directrices y procedimientos de seguridad: auditorías y revisiones periódicas; simulacros de fallos y ataques informáticos; inspección manual de los procedimientos y tareas realizadas día a día por el personal; utilización de herramientas para detectar violaciones de la seguridad (intentos de acceso a carpetas y documentos protegidos, contraseñas poco robustas o instalación de software no autorizado en los equipos de la organización, por citar algunas de las más frecuentes); cuestionarios y entrevistas al personal para determinar su nivel de sensibilización y conocimiento de las Políticas; etcétera.

Otra medida que contribuye a una adecuada implantación sería la actualización y revisión de las Políticas de Seguridad cuando sea necesario, manteniendo plenamente vigentes las directrices y medidas establecidas.

Las posibles violaciones de las Políticas de Seguridad pueden tener lugar por

desconocimiento o falta de la adecuada formación, por negligencia, por un fallo accidental o bien por una actuación malintencionada de un determinado usuario del sistema. Como consecuencia de estas violaciones de las directrices y medidas de seguridad, la organización deberá determinar cuál es el nivel de responsabilidad del usuario y de la gravedad de su actuación, adoptando las correspondientes medidas disciplinarias que correspondan en cada caso.

Las medidas disciplinarias tendrían que haber sido previamente aprobadas y publicitadas por la Dirección o el Departamento de Recursos Humanos, contando con la participación de los propios representantes de los trabajadores. Estas medidas disciplinarias deberían ser consecuentes con el resto de las políticas de la empresa, respetando además los derechos fundamentales de los trabajadores y la legislación laboral vigente.

7. AUDITORÍA DE LA GESTIÓN DE LA SEGURIDAD

La Auditoría de la Gestión de la Seguridad constituye un elemento fundamental dentro de las Políticas de Seguridad, ya que cumple con el objetivo de poder verificar de forma periódica la correcta configuración de los equipos y el nivel de implantación de las Políticas y Procedimientos de Seguridad definidos por la organización, así como la adecuación de éstas a las nuevas necesidades y características del sistema informático de la organización.

En este sentido, sería conveniente que la auditoría se realizase de acuerdo con las guías y recomendaciones de organismos reconocidos a nivel nacional e internacional, como ISACA (*Information Systems Audit and Control Association*, www.isaca.org).

Podemos considerar las siguientes etapas en una auditoría:

1. Planificación de la auditoría (tareas a realizar y recursos necesarios), definiendo el ámbito y los objetivos perseguidos. Asimismo, será necesario proceder a la validación de estos objetivos con los dueños y responsables del sistema.
2. Realización de las tareas planificadas, documentando cada una de estas tareas y los resultados obtenidos.
3. Validación de los resultados de la auditoría.
4. Elaboración del informe con los resultados de la auditoría, las conclusiones y recomendaciones.
5. Presentación y aprobación de la auditoría por parte de los dueños y responsables del sistema.

En todo este proceso conviene destacar la importancia de mantener la seguridad de los registros de auditoría ("*audit trails*"), que facilitan el seguimiento de la actividad en los sistemas que van a ser auditados.

REFERENCIAS BIBLIOGRÁFICAS

S. Barman, Writing Information Security Policies, New Riders Publishing, 2001.

E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, 2004.

E. Cole, R. Krutz, J. Conley, Network Security Bible, John Wiley & Sons, 2005.

C. Cresson, Information Security Policies Made Easy, PentaSafe Security Technologies, 2002.

J. Erickson, Hacking: The Art of Exploitation, No Starch Press, 2003.

A. Gómez, Enciclopedia de la Seguridad Informática, Ra-Ma, 2006.

K. Mitnick, W. Simon, The Art of Intrusion, John Wiley & Sons, 2005.

RFC's 1244, 2196 y RFC 3067.

R. Russell, Stealing the Network: How to Own the Box, Syngress, 2003.

J. Scambray, S. McClure, G. Kurtz, Hacking Exposed: Network Security Secrets & Solutions - 2nd Edition, Osborne/McGraw-Hill, 2001.

J. Scambray, M. Shema, Hacking Exposed Web Applications, Osborne/McGraw-Hill, 2002.

RESEÑA CURRICULAR DEL AUTOR

Álvaro Gómez Vieites

Ingeniero de Telecomunicación por la Universidad de Vigo. Especialidades de Telemática y de Comunicaciones. Número uno de su promoción (1996) y Premio Extraordinario Fin de Carrera.

Ingeniero Técnico en Informática de Gestión" por la UNED (2004-2006). Premio al mejor expediente académico del curso 2004-

2005 en la Escuela Técnica Superior de Ingeniería Informática de la UNED

"Executive MBA" y "Diploma in Business Administration" por la Escuela de Negocios Caixanova.

Ha sido Director de Sistemas de Información y Control de Gestión en la Escuela de Negocios Caixanova. Profesor colaborador de esta entidad desde 1996, responsable de los cursos y seminarios sobre Internet, Marketing Digital y Comercio Electrónico.

Socio-Director de la empresa SIMCe Consultores, integrada en el Grupo EOSA.

Autor de varios libros y numerosos artículos sobre el impacto de Internet y las TICs en la gestión empresarial.