UNE-ISO/IEC 27001

Más seguridad para la era SMAC

Las tecnologías de la información están viviendo una nueva revolución denominada SMAC, por las siglas en inglés de social, móvil, analíticas y la nube. La seguridad, en esta nueva era, sigue siendo una cuestión crucial y por ello la certificación según la ISO 27001 es un eficaz aliado para los CIO *(Chief Information Officer)* y los CISO *(Chief Information Security Officer)*. España acaba de adoptar como norma nacional la versión de 2013, que entre otras cuestiones presta una mayor atención al contexto de las organizaciones y a los objetivos y riesgos de seguridad.

Carlos Manuel Fernández
Boris Delgado
Gerencia de TIC AENOR

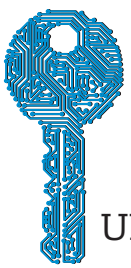
El vertiginoso desarrollo que han experimentado las tecnologías de la información y la comunicación ha sido crucial para la modernización del tejido empresarial y las administraciones públicas de muchos países. Actualmente, las TIC viven una nueva revolución que viene determinada por la generalización del uso de la tecnología móvil y las redes sociales, y que está conllevando un despliegue de las tecnologías conocidas como SMAC (por las siglas en inglés de social, móvil, analíticas y la nube). En este contexto, ahora más que nunca, asegurar la confidencialidad, integridad y disponibilidad de un sistema de información es crucial.

En el *World Economic Forums Annual* de 2014 celebrado en Davos, la aseguradora SWISS RE presentó las conclusiones de un estudio realizado

Tabla 1.Comparativa del número de controles por dominio

ANEXO I ISO 27001:2005. Dominio		TOTAL CONTROLES
A5	• Política de Seguridad	2
A6	• Aspectos organizativos de la seguridad de la información	11
A7	• Gestión de Activos	5
A8	• Seguridad ligada a los RRHH	9
A9	• Seguridad física y ambiental	13
A10	• Gestión de comunicaciones y operaciones	32
A11	• Control de acceso	25
A12	• Adquisición, desarrollo y mantenimiento de los sistemas de información	16
A13	• Gestión de incidentes de seguridad de la información	5
A14	• Gestión de la continuidad de negocio	5
A15	• Cumplimiento	10
	Total	133

ANEXO I ISO 27001:2013. Dominio		TOTAL CONTROLES
A5	• Políticas de Seguridad de la Información	2
A6	• Organización de la seguridad de la información	7
A7	• Seguridad relativa a los RRHH	6
A8	• Gestión de activos	10
A9	• Control de acceso	14
A10	• Criptografía	2
A11	• Seguridad física y del entorno	15
A12	• Seguridad en las operaciones	14
A13	• Seguridad en las comunicaciones	7
A14	• Adquisición, desarrollo y mantenimiento de los sistemas de información	13
A15	• Relación con proveedores	5
A16	• Gestión de incidentes de seguridad de la información	7
A17	• Aspectos de seguridad de la información en continuidad de negocio	4
A18	• Cumplimiento	8
	Total	114



UNE-ISO/IEC 27001

a través de más de 700 entrevistas a ejecutivos de Estados Unidos, Francia, Alemania, Italia, Japón y Reino Unido sobre la valoración de riesgos económicos, ambientales, geopolíticos, sociales y tecnológicos. Según el estudio, los riesgos tecnológicos son de máxima prioridad siendo los tres más identificados: fraude, robo de información y de datos; daños o pérdidas de información de las infraestructuras críticas, y ciberataques.

Para afrontar este reto, más de 22.000 organizaciones de 105 países confían en la Norma ISO 27001 de Sistemas de Gestión de Seguridad de la Información como herramienta eficaz que les ayuda a implantar los controles adecuados. Publicada por primera vez en 2005, esta norma fue revisada el pasado año, teniendo en cuenta las experiencias de quienes la vienen utilizando desde entonces, y acaba de adoptarse como norma española.

La Asociación Española de Empresas de Electrónica, Tecnologías de la Información y Comunicación (AMETIC), en un reciente estudio sobre la ISO 27001, destaca la satisfacción y la alta valoración de las direcciones generales, personal, clientes y proveedores de aquellas empresas que han implantado y actualmente mantienen el Sistema de Gestión de Seguridad de la Información según la Norma ISO/IEC 27001.

Novedades

La nueva versión de la norma adopta la llamada Estructura de Alto Nivel utilizada en todas las normas de sistemas de gestión, lo que facilita su integración con otros sistemas, como calidad, medio ambiente o seguridad y salud en el trabajo, de forma más sencilla. De acuerdo con esta estructura, la UNE-ISO/IEC 27001:2014 pide a las organizaciones que profundicen más su conocimiento sobre el contexto en el que operan y las necesidades de las partes interesadas. Igualmente, otorga mayor importancia a la definición de objetivos de seguridad. La norma identifica áreas o dominios a los que asocia uno o varios objetivos de seguridad. A su vez, por cada objetivo se definen uno o más controles de seguridad cuya implantación debe traducirse en la consecución del objetivo de seguridad asociado. Otra de las diferencias frente a la versión anterior es que la norma refuerza la mejora continua, basándose en un ciclo de planificación, ejecución, monitorización y mejora donde el ciclo PDCA encaja perfectamente.

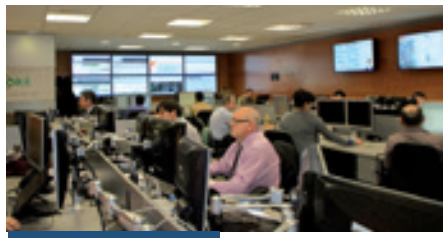
El Sistema de Gestión de Seguridad de la Información sigue en la línea de preservar la confidencialidad, integridad y disponibilidad de los procesos

Las organizaciones deben profundizar más en su conocimiento sobre el contexto en el que operan y las necesidades de las partes interesadas

de negocio/activos de información mediante la aplicación de un proceso de gestión de riesgos, y otorga a las partes interesadas confianza sobre la adecuada gestión de los riesgos. Esta nueva versión de la norma no determina cómo se evalúan los riesgos y se alinea con la ISO 31000, referencial de gestión de riesgos globales.

Riesgos

En la nueva UNE-ISO/IEC 27001:2014 se consideran riesgos y oportunidades de mejora para las incidencias de seguridad, minimizando los riesgos y amenazas en los sistemas de información. Se pone en valor la nueva figura "dueño del riesgo" con la responsabilidad suficiente para aprobar el riesgo residual y el plan de tratamiento del riesgo. Recordemos que en la selección de controles que hay que aplicar y el plan de tratamiento de riesgo debe existir un equilibrio de acuerdo a la máxima: riesgo vs control vs coste. Al fin y al cabo, hay que buscar la mayor eficiencia, eficacia y economía en la aplicación de la seguridad de la información siempre orientada a los objetivos del negocio.



EXPERIENCIAS

Mejor gestión del riesgo

Pedro Muñoz
Director de la División de Tecnología de Sistemas Informática El Corte Inglés (España)

En Informática El Corte Inglés, proveedor de consultoría tecnológica, soluciones TIC y servicios de *Outsourcing*, como parte de nuestra estrategia y compromiso de ofrecer las máximas garantías de calidad en productos y servicios a los clientes, apostamos por la calidad en la gestión, implantando buenas prácticas y certificándolas acorde a requisitos recogidos en estándares internacionales.

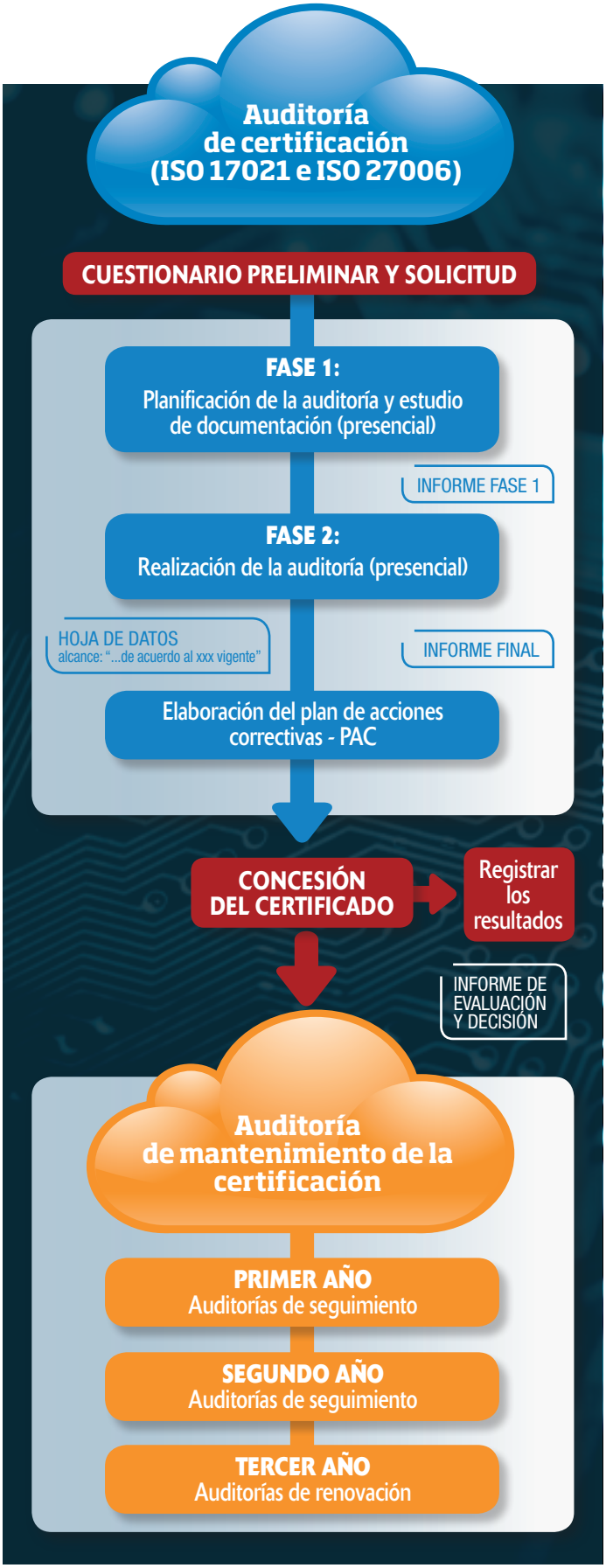
En esta línea, recientemente hemos acometido la adaptación de nuestro Sistema de Gestión a la Norma ISO/IEC 27001:2013, lo cual se ha llevado a cabo en un año de trabajo en el que abordamos la revisión de todos los procedimientos de Seguridad de la Información.

Disponíamos de dos sistemas de gestión, uno que integraba los requisitos de las Normas UNE-EN ISO 9001 y UNE-ISO/IEC 20000-1; y otro para la Seguridad de la Información según la UNE-ISO/IEC 27001:2007. Gracias a la modificación de la versión 2013, que sigue las pautas marcadas por el Anexo SL, ambos han podido ser integrados en uno solo.

Adicionalmente, el cambio de enfoque de gestión de riesgos de la nueva norma -que deja de estar basado en activos, amenazas y vulnerabilidades- nos ha permitido simplificar la gestión extraordinariamente, unificando en una sola metodología las dos anteriores; una para los riesgos de seguridad de la información de acuerdo a la anterior ISO 27001, y otra de tratamiento de riesgos "por servicio", acorde a la Norma ISO 20000-1. Igualmente hemos podido articular el concepto de "Dueño del Riesgo", asignando cada riesgo a aquella persona que realmente lo conoce y puede valorar su impacto, responsabilizándose de hacer todo lo posible para evitar su ocurrencia y mitigar las consecuencias en caso de llegar a materializarse, consiguiendo una gestión de riesgos muy dinámica.

El esfuerzo realizado se ha visto compensado, pues los cambios introducidos simplifican la gestión, ahorrando costes.

Proceso de certificación con la UNE-ISO/IEC 27001:2014



UNE-ISO/IEC 27001

Principales novedades de la UNE-ISO/IEC 27001:2014

- Aplicación de la estructura de alto nivel de ISO - Anexo SL.
- Refuerzo en un sistema de gestión basado en la mejora continua.
- Mayor consideración y relevancia al contexto de la organización, al liderazgo y compromiso de la Dirección, y a las necesidades de las partes interesadas.
- Mayor relevancia a la definición y seguimiento de objetivos de seguridad de la información.
- Asignación de autoridad y responsabilidades al dueño del riesgo.
- Proceso de análisis de riesgos más general alineado con la ISO 31000, considerando riesgos y oportunidades.
- Reestructuración (nuevos, modificados, eliminados) de los controles del Anexo A. ISO 27001 (ISO 27002) quedando en un total de 114 de los 133 anteriores.

CURSOS Y PUBLICACIONES DE AENOR RELACIONADAS

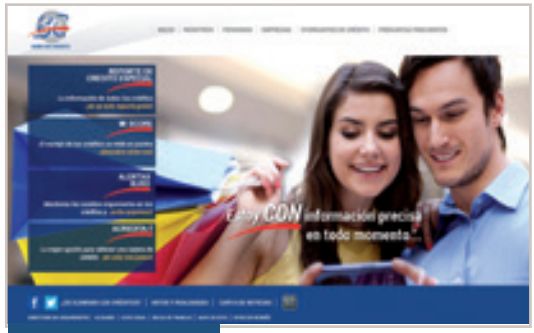
- Cambios en las Normas ISO 27001 e ISO 27002. Repercusión en un SGSI
- Fundamentos de la gestión de la seguridad de la información según ISO 27002
- Implantación de un sistema de gestión de seguridad de la información según ISO 27001
- Auditoría de sistemas de gestión de seguridad de la información según ISO 27001
- Gestión de riesgos en seguridad de la información
- Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. 2.ª edición
- Modelo para el gobierno de las TIC basado en las normas ISO

La norma identifica áreas o dominios a los que asocia uno o varios objetivos de seguridad. A su vez, por cada objetivo se definen uno o más controles de seguridad cuya implantación debe traducirse en la consecución del objetivo de seguridad asociado

Con respecto a los objetivos de control y controles, la tabla 1 indica el número de controles por dominios donde se puede apreciar una reestructuración (nuevos, modificados, eliminados) de los controles del Anexo A. ISO 27001 (ISO 27002) quedando en total 114 controles con respecto a los 133 controles anteriores de la ISO/IEC 27001:2005.

El proceso de certificación es el mismo que para la anterior versión de la ISO/IEC 27001:2005, siguiendo las normas internacionales en las que AENOR está acreditada -ISO/IEC 17021 e ISO 27006-. Las organizaciones certificadas según la versión de 2005 deberán iniciar la transición hacia la nueva versión para que sus certificados sigan en vigor. AENOR ya ha realizado más de diez auditorías de certificación contemplando la nueva versión de la ISO/IEC 27001 y comprobando que las organizaciones se han adaptado adecuadamente a esta nueva versión de la norma.

En definitiva, la nueva versión de la UNE ISO/IEC 27001:2014 contempla una mayor orientación hacia la ciberseguridad y los ciberriesgos, tanto en el mundo de la gestión empresarial (ISO 27001-ISO 27002) como en el ámbito de los procesos industriales (ISO 27001-SCADA). Actualmente, AENOR tiene vigentes cerca de 300 certificados según la Norma ISO 27001.



EXPERIENCIAS

Referencia internacional

René Salinas
CIO
Buró de Crédito
(México)

Buró de Crédito es una empresa con la misión de ofrecer soluciones a otorgantes de crédito y consumidores (público) para la administración del riesgo crediticio. Para ello cuenta con un amplio catálogo de productos y servicios que ofrece, principalmente, a través del uso de tecnología.

Hoy en día, nuestras operaciones son reguladas por una Ley Federal -Ley para regular las Sociedades de Información Crediticia (SIC)-, y por Reglas Generales para SIC emitidas por el Banco de México. Es por esto, y por la sensibilidad de la información que administramos, que es indispensable considerar en nuestras operaciones la confidencialidad, integridad y disponibilidad de la información.

Para resolver esta necesidad, Buró de Crédito implantó desde hace más de ocho años la Norma ISO 27001 (antes ISO 17799) como un marco de referencia formal y de mejores prácticas en el ámbito internacional en materia de Seguridad de la Información.

La implantación de esta norma de Gestión de Seguridad de la Información nos ha apoyado no sólo en los riesgos informáticos, sino también en el proceso integral de administración de riesgos de la empresa. Asimismo, hemos cubierto, a través de un proceso formal y estandarizado, las necesidades de Seguridad de la Información.

Es importante subrayar que las actualizaciones que ha tenido la norma han sido de utilidad para Buró de Crédito, ya que la adopción de nuevos productos y servicios, esquemas de operación e implementación de nuevas tecnologías trae consigo nuevas amenazas a la Seguridad de la Información. Contar con esta certificación ha sido esencial para mantenernos al día en los controles de seguridad que hemos ido implementado, con el objetivo de ofrecer un mejor servicio y con aún más calidad. Además, permite brindar confianza a los clientes y usuarios sobre el uso y control de la información.