CASOS PRÁCTICOS

La empresa valenciana S2 Grupo presta servicios de ciberseguridad a administraciones públicas y grandes empresas del Ibex 35. A los certificados de sistemas de gestión según ISO/IEC 27001, ISO 20000-1, ISO 9001, ISO 14001 y UNE 166002 acaba de unirse el del Esquema Nacional de Seguridad de categoría alta. Para ello, entre otras cuestiones, la empresa ha implantado sistemas cortafuegos de diferentes fabricantes y dos factores de autenticación con caducidad de credenciales.

S2 Grupo, ciberseguridad certificada

Alberto Olmos
Director de Gestión
S2 Grupo

S2 Grupo es una empresa valenciana con proyección internacional especializada en ciberseguridad de entornos empresariales e industriales y en explotación de sistemas de misión crítica. Entre sus clientes se encuentran las principales administraciones públicas y grandes empresas (muchas de las cuales cotizan en el IBEX-35), así como numerosas empresas de tamaño medio. Cuenta con oficinas en Madrid, Barcelona, Valencia, Bruselas, Bogotá y Mexico D.F. y su Centro de Servicios, S2 Grupo CERT, engloba un Centro de Operaciones de Seguridad (SOC), un Centro de Operaciones de Seguridad Industrial (iSOC) y un Centro de Explotación (NOC) desde el que se proveen servicios las 24 horas de los 365 días del año.

S2 Grupo invierte aproximadamente entre el 15 y el 20 % de sus ingresos anuales en I+D+i y cuenta con expertos altamente cualificados en las distintas ramas de la ciberseguridad (técnica, organizativa, física y legal) necesarios en una estrategia multidisciplinar para ofrecer soluciones integrales.

Cuenta con una suite propia de productos entre los cuales se encuentra CARMEN, la capacidad nacional de detección de APT (Amenazas Persistentes Avanzadas) y una de las pocas herramientas globales para la detección de ciberataques avanzados y compromisos por APT. Es tecnología 100 % desarrollada en España en colaboración con el Centro Criptológico Nacional (CCN), adscrito al Centro Nacional de Inteligencia.

Experiencia en sistemas de gestión

La compañía fue pionera en España en la implantación de Sistemas de Gestión de Seguridad de la Información (SGSI), ya que fue la empresa que prestó, en el año 2005, servicios de consultoría a la primera organización en certificar su SGSI conforme a la Norma UNE 71502, precursora de la actual ISO 27001.

A comienzos de 2006, S2 Grupo certificó su propio SGSI. Posteriormente fue sumando nuevos certificados según las Normas ISO 9001 de gestión de la calidad, ISO 20000-1 de gestión TI de su Centro de Servicios, UNE 166002 de gestión de la I+D+i e ISO 14001 de gestión ambiental. A estas certificaciones hay que añadir el certificado de conformidad con el Esquema Nacional de Seguridad (ENS), con categoría alta, conforme a las exigencias del Real Decreto 3/2010 conseguido el pasado mes de julio, tras superar la correspondiente auditoría. Los alcances de las certificaciones de S2 Grupo abarcan todos los servicios de ciberseguridad prestados.

Cuando se incorporan requisitos de distintos referenciales a un sistema de gestión empresarial no tiene ningún sentido hacerlo de manera aislada. Porque de hacerse así, podríamos

desaprovechar sinergias entre requisitos idénticos o parecidos de distintas normas e incurrir en costes innecesarios por duplicidad o solape de procesos, actividades y registros e incluso en incongruencias. Esto siempre fue así pero cobró aún mayor sentido desde que en 2013, por fin, se alinearan los requisitos comunes a todas las normas ISO de sistemas de gestión bajo una estructura común, lo que facilitó mucho la integración y la auditoría de los mismos.

Consecuentemente, S2 Grupo dispone de un único sistema de gestión compuesto por aproximadamente cien documentos (entre procesos y procedimientos operativos) que integra los requisitos de las cinco normas indicadas anteriormente. Y ahora también los del ENS.

La incorporación de las exigencias de seguridad del ENS al Sistema de Gestión Integrado (SGI) se ha realizado, lógicamente, a través del SGSI y ha sido conceptualmente muy simple: se han considerado las medidas de seguridad del ENS como una extensión de los controles de seguridad recogidos en el anexo A de la Norma ISO/IEC 27001. Este enfoque encaja perfectamente con la primera nota del apartado 6.1.3 de la norma *Tratamiento de los riesgos de seguridad de la información* que indica que *"las organizaciones pueden diseñar controles según sea necesario, o identificarlos a partir de cualquier fuente"*. Así pues, a los 114 controles de seguridad recogidos por el famoso anexo A se han añadido las exigencias del ENS no contempladas en la Norma ISO/IEC 27001.

S2 Grupo dispone de un único sistema de gestión, compuesto por cerca de 100 documentos, que integra los requisitos de ENS, ISO/IEC 27001, ISO 20000, ISO 9001, UNE 166002 e ISO 14001

Esta simplicidad ha sido más bien conceptual, ya que el enfoque aplicado no resta dificultad a una disciplina intrínsecamente compleja como es la ciberseguridad. Ésta abarca distintas y variadas áreas de conocimiento, algunas de ellas ciertamente complejas como desarrollo y administración de sistemas, seguridad lógica, comunicaciones, *compliance* legal, criptografía, etc.

Por fortuna un buen número de las medidas de seguridad requeridas por el ENS ya estaban contempladas en mayor o menor medida por la Norma ISO/IEC 27001, lo que vino a *suavizar* en parte dicha dificultad.

Para conocer el nivel de solape entre la norma y ENS resulta de gran ayuda la *Guía de Seguridad de las TIC. CCN-STIC 825. Esquema Nacional de Seguridad. Certificaciones 27001,* publicada por el CCN. Ésta ▶▶

Tabla 1

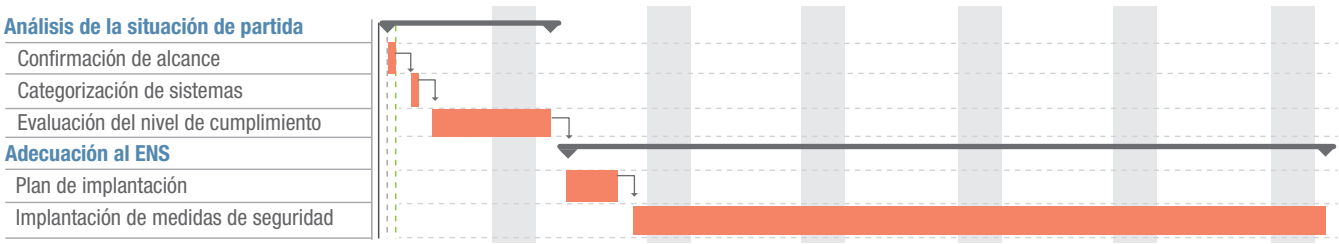
Relación entre medidas del ENS y controles de ISO 27001

Nivel	Significado	Número de medidas	Porcentaje
0	Cubierto por la Norma ISO 27001	33	44 %
1	Probablemente cubierto	27	36 %
2	Probablemente se necesite completar	6	8 %
3	No cubierto por la Norma ISO 27001	9	12 %
	TOTAL	75	100 %

Fuente: Guía de Seguridad de las TIC. CCN-STIC 825. Esquema Nacional de Seguridad. Certificaciones 27001.

Tabla 2

Fases de proyecto



CASOS PRÁCTICOS

contiene una tabla que, basándose en un esquema de cuatro niveles, recoge una estimación del grado de cumplimiento del ENS que cabe esperar a partir de un SGSI conforme a ISO 27001. (Tabla 1)

Simplificando mucho podríamos considerar que aproximadamente el 80 % de las medidas de seguridad del ENS quedan cubiertas o casi cubiertas (niveles 0 y 1) por la Norma ISO 27001, lo cual no es poco.

En S2 Grupo en total se han revisado los 66 controles correspondientes a los tres primeros niveles, haciendo hincapié en los controles de nivel 2, y se han incorporado las nueve medidas novedosas aportadas por el ENS como controles adicionales.

Fases del proyecto

El proyecto de adecuación al ENS en S2 Grupo se abordó en dos fases (ver tabla 2). La primera de ellas consistió en una fase diagnóstica en la que se confirmó el alcance de sistemas y servicios (la totalidad de los sistemas de información y de la cartera de servicios de ciberseguridad), se revisó la categorización de los sistemas y se realizó una evaluación del nivel de cumplimiento para determinar el delta faltante. La segunda fase, la propia de adecuación (plan de implantación, despliegue de las novedades aportadas por el ENS), consumió una buena cantidad de recursos a lo largo de varios meses.

Los más de diez años de rodaje del SGSI, por un lado, y la experiencia de S2 Grupo en implantaciones del ENS, por otro, han permitido simplificar en parte el proyecto de adecuación con respecto a otros proyectos desarrollados en clientes.

No es el ENS un texto de lectura fácil; ni la ciberseguridad, como ya se indicó, una materia sencilla, más bien al contrario. Consecuentemente, el proceso de auditoría de las exigencias del ENS, ya sea interno o externo, tampoco resulta sencillo. Además de los conocimientos y experiencia exigibles a todo auditor (técnicas de auditoría, capacidad de análisis, expresión escrita, etc.), en el caso del ENS resulta imprescindible un buen conocimiento de la materia y muchas horas de vuelo en tecnologías de la información en general, en ciberseguridad en particular, en las Normas ISO 27001, 27002 y afines, y en el propio ENS. Estos requisitos tan específicos resultan inexcusables, en mi opinión, para que el auditor pueda desarrollar su trabajo con solvencia, lo que desde el punto de vista de la empresa se gradece y mucho.

Con independencia de todo ello y aunque el parecido entre el texto legal y una norma ISO es *a priori* escaso, el proceso de auditoría tanto interna como externa sí es muy similar al de las auditorías de sistemas de gestión.

ENS versus Sistemas de Gestión

El propio Real Decreto 3/2010 indica que "concibe la seguridad como una actividad integral" pero obviamente no establece requisitos de un sistema de gestión si no que "se limita a establecer los principios básicos y requisitos mínimos que […] permiten una protección adecuada de la información y los servicios".

S2 Grupo: 2017 en cifras			
11 M	18%	240	1,3M
Facturación	Crecimiento promedio	Empleados	Inversión en I+D+i




Cerca del 80 % de las medidas de seguridad del ENS quedan cubiertas, o casi cubiertas, por la ISO/IEC 27001, si bien el ENS requiere nueve medidas nuevas muy concretas

Al integrarse en el SGI de S2 Grupo las exigencias del ENS heredan automáticamente la capa de gestión que esa "actividad integral" del ENS pasa casi de soslayo, quedando incluidas en los procesos normales de seguimiento, auditoría, revisión, mejora continua, etc. de cualquier sistema de gestión.

Cabe mencionar, en claro contraste con las normas ISO en general, la concreción de algunas de las exigencias del ENS como, por ejemplo, para nivel alto, la obligatoriedad de disponer de sistemas cortafuegos de diferente fabricante dispuestos en cascada y redundantes; la exigencia de disponer de, al menos, dos factores de autenticación con caducidad de credenciales, o la necesidad de utilizar sistemas, productos o equipos con certificación *Common Criteria*. Estos requisitos no son en absoluto triviales de cumplir y pueden conllevar inversiones importantes en ocasiones.

Por fortuna, la inicial rigidez inherente al texto legal queda en parte suavizada por las medidas compensatorias contempladas en el punto 5 del artículo 27 del mismo. Éste establece que las medidas de seguridad exigidas por el ENS pueden ser reemplazadas por otras medidas compensatorias, siempre y cuando se justifique documentalmente que el nivel de protección es equivalente o superior, y cuente con una aprobación expresa por parte del responsable de seguridad de la organización, lo cual permite, agudizando el ingenio, un cierto margen de maniobra.

El Centro Criptográfico Nacional ha desarrollado un buen número de guías relacionadas con el ENS, algunas de las cuales pueden resultar particularmente útiles, como la mencionada CCN-STIC 825. ◗