S2 GRUPO

Protección de infraestructuras críticas

3er Informe Técnico
marzo 2014


S2
GRUPO

ÍNDICE

1 Introducción

Este documento continúa la línea de trabajo iniciada en 2011, año en el que publicábamos nuestro primer Informe sobre Protección de Infraestructuras Críticas, en el que analizábamos la situación internacional y nacional en la materia –principalmente normativa- y planteábamos las líneas de trabajo a desarrollar para seguir lo que estimamos es la dirección correcta en el ámbito de la PIC. Aquel primer trabajo tuvo su continuación en 2012 con un segundo informe sobre la PIC en España, en este caso mucho más práctico y con un objetivo concreto: determinar si las infraestructuras críticas pueden considerarse "inseguras" en España (y si es posible, cuántas y de qué sectores) desde un punto de vista operativo.

En esta ocasión continuamos con este enfoque práctico de nuestro último informe y nos centramos en un punto que juzgamos que es de capital importancia y que, sin embargo, no recibe la atención que en nuestra opinión merece: la disponibilidad de información detallada sobre nuestras II.CC. libremente accesible a través de internet, especialmente en lo referente a sus instalaciones, procesos, sistemas de control, procedimientos de operación y, por último, organización y gestión de la seguridad.

Dada la diversidad de II.CC. en cuanto a sectores, titularidad, modo de gestión, etc. es importante definir una metodología de estudio que permita afrontar el trabajo de modo manejable pero a la vez suficientemente representativo, acotando el campo de búsqueda. Nuestro objetivo final es conseguir:

- Descubrir qué tipo de información está disponible en internet acerca de nuestras II.CC.
- Determinar el origen de la información.
- Estimar el grado de riesgo que puede suponer el uso de la información hallada por parte de un atacante.
- Establecer si existe alguna diferencia entre los distintos subsectores en que se divide el conjunto de II.CC.
- Analizar los resultados obtenidos para dibujar un cuadro general que nos permita avanzar conclusiones al respecto.

Independientemente de que la seguridad por oscuridad no es una opción válida, no debe olvidarse que, del mismo modo que el primer paso en un ataque es la recopilación de información, el primer paso de una estrategia de defensa debe ser el control de la misma.

2 Metodología

Nuestra aproximación ha consistido en seleccionar una organización englobada en uno de los sectores estratégicos y buscar información sobre ella en internet. La Ley 8/2011 define en su anexo los sectores estratégicos españoles y los Organismos o Ministerios competentes en cada caso (con los correspondientes cambios de denominación que hayan sufrido desde la publicación de la Ley hasta ahora):

Sector	Ministerio/Organismo del sistema
Administración.	Ministerio Presidencia. Ministerio Interior. Ministerio Defensa. Centro Nacional de Inteligencia. Ministerio Política Territorial y Administración Pública.
Espacio.	Ministerio Defensa.
Industria nuclear.	Ministerio Industria, Turismo y Comercio. Consejo de Seguridad Nuclear.
Industria química.	Ministerio Interior.
Instalaciones de investigación.	Ministerio Ciencia e Innovación. Ministerio Medio Ambiente, y Medio Rural y Marino.
Agua.	Ministerio Medio Ambiente, y Medio Rural y Marino. Ministerio Sanidad, Política Social e Igualdad.
Energía.	Ministerio Industria, Turismo y Comercio.
Salud.	Ministerio Sanidad, Política Social e Igualdad. Ministerio Ciencia e Innovación.
Tecnologías de la Información y las Comunicaciones (TIC).	Ministerio Industria, Turismo y Comercio. Ministerio Defensa. Centro Nacional de Inteligencia. Ministerio Ciencia e Innovación. Ministerio Política Territorial y Administración Pública.
Transporte.	Ministerio Fomento.
Alimentación.	Ministerio Medio Ambiente, y Medio Rural y Marino. Ministerio Sanidad, Política Social e Igualdad. Ministerio Industria, Turismo y Comercio.
Sistema financiero y tributario.	Ministerio Economía y Hacienda.

En esta investigación nos hemos centrado en aquellos sectores en los cuales se hace un uso destacado de sistemas de control industrial, dejando para una entrega posterior el resto. Así pues, de la relación establecida en la Ley hemos excluido los sistemas financiero y tributario, las TIC y las instalaciones de investigación. De esta forma, el objeto de este informe se centra en:

- Sector sanitario
- Energía
- Trasporte
- Industria química
- Industria nuclear
- Abastecimiento de agua
- Alimentación
- Administración
- Sector aeroespacial

Se han realizado búsquedas en internet para tratar de localizar información asociada a las organizaciones seleccionadas. En particular:

1. Relativa a equipos electromecánicos, instalaciones, obra civil o edificación, etc.: marcas, modelos, fotografías, manuales, etc.

2. Relativa a componentes del sistema de control industrial: marcas, modelos, arquitectura, protocolos, configuración, software, etc.

3. Relativa al proceso: planos, diagramas, memorias, manuales de operación, etc.

4. Relativa a activos o procesos TIC.

5. Relativos a la seguridad: seguridad física, seguridad lógica,…

Podría argüirse que restringir la búsqueda a una única organización por sector supone un sesgo excesivo. En nuestra opinión, y teniendo en cuenta el carácter cualitativo de nuestro estudio, esto no es así, ya que otros factores contrarrestan esta aparente limitación.

En primer lugar, se han seleccionado objetivos cuya dimensión les convierte en muy apetecibles por la repercusión que un ataque exitoso tendría o por el valor de la información que estas organizaciones manejan.

En segundo lugar porque, al ser líderes en sus sectores, constituyen casos a imitar por terceros.

En tercer lugar porque, con frecuencia, las organizaciones de un sector comparten estrategias, historia y marco regulador, lo que hace que existan patrones de comportamiento comunes.

En último lugar porque, aunque el objetivo de la búsqueda esté definido de antemano, la propia naturaleza de los buscadores hace que se encuentre información relativa a otras empresas del mismo sector, lo que permite verificar si es posible extrapolar las conclusiones para darles un valor general.

Una vez finalizada la etapa de búsqueda, se ha clasificado la información obtenida en función de los siguientes criterios:

- El tipo de información.
- El contexto en el que está contenida.
- El origen.
- La consideración subjetiva del impacto que podría suponer el uso de esta información.

Se han establecido tres niveles: bajo, medio y alto.

En ocasiones, la primera idea no ha resultado fructífera (es decir, no se ha hallado un número suficiente de documentos como para extraer conclusiones). En tales casos se ha buscado una alternativa con un mismo nivel de representatividad.

Por último, se ha asignado a cada sector una valoración subjetiva global de la percepción obtenida de la facilidad o dificultad, según corresponda, para obtener información sensible.Los resultados de la campaña se han organizado en tablas y se presentan de forma anónima.

Insistimos en que la idea detrás de esta investigación no es realizar una campaña exhaustiva de localización de información, algo que, por otra parte, es casi imposible, sino obtener una visión cualitativa de la magnitud del problema, sus causas y posibles soluciones.

Las búsquedas en Internet se han llevado a cabo en el periodo comprendido entre el mes de noviembre de 2013 y el mes de febrero de 2014.

Por último, cabe indicar que la existencia de la información localizada se ha puesto en conocimiento de las entidades y organismos con competencias en materia de ciberseguridad.

3 Resultados Obtenidos

La siguiente tabla recoge los resultados de la investigación.

SECTOR	TIPO INFORMACIÓN	ORIGEN	IMPACTO POSIBLE DE LA INFORMACIÓN	PERCEPCIÓN SUBJETIVA SECTOR (FACILIDAD DE LOCALIZAR INFO.)
SANITARIO	Proyecto obras	Interno	Bajo	Difícil
ENERGÍA	Proyectos, PFC, declaraciones ambientales, PPS, documentos divulgación,	Interno, universidades	Medio	Medio
TRANSPORTE	PFC, artículos técnicos, casos éxito, PPS, divulgación	Interno, universidades, proveedores, empleados	Medio	Medio
INDUSTRIA QUÍMICA	PFC	Universidades	Alto	Fácil
INDUSTRIA NUCLEAR	Artículos técnicos, casos éxito, pliegos	Interno	Medio	Difícil
AGUA	PFC, pliegos, artículos técnicos	Interno, universidades	Alto	Fácil
ALIMENTACIÓN	Pliegos, casos éxito	Interno, proveedores	Alto	Fácil
ADMINISTRACIÓN	Pliegos, documentos técnicos	Interno	Medio	Fácil
AEROESPACIAL	(1)	(1)	(1)	Difícil

(1) No se ha localizado información sensible relacionada con el sector espacial. Explicación en el texto.

4

Discusión y Análisis

4.1 Tipo de información

El formato en el que aparece la información es bastante variado, aunque existen algunas categorías que acaparan la mayor parte de los resultados:

• Proyectos fin de carrera (PFC) y tesis doctorales.

Es sorprendente la cantidad de información detallada que puede encontrarse en estos documentos. La colaboración entre universidades y empresas encuentra en este tipo de acciones un elemento fundamental en que ambas partes se benefician. Lo mismo puede decirse de los alumnos, que en muchos casos consiguen empleo o, cuando menos, una beca, en la empresa colaboradora. En muchos casos, los departamentos de las empresas no consideran los PFC documentos destinados a salvar un mero trámite por parte del alumno, sino como medio para tratar cuestiones de importancia con el respaldo científico de un departamento universitario. De este modo se encuentran en la red PFC que desarrollan asuntos clave, detallando pruebas de concepto o, incluso, constituyéndose en la base de un esfuerzo normalizador. De hecho hemos localizado incluso un PFC que versa sobre el diseño de una subestación de distribución de energía eléctrica desarrollado dentro del departamento de normalización de una compañía eléctrica.

En otros casos, los PFC se aprovechan para resolver cuestiones de ingeniería específicas, es decir, para definir instalaciones o sistemas destinados a construcción. Ello, además, con el agravante que supone la minuciosidad en el detalle que caracteriza a este tipo de ejercicios académicos. En esta línea hemos encontrado un PFC que diseña el sistema de control de un sistema de deslastre de cargas eléctricas de una industria de primera magnitud.

• Pliegos de concursos públicos.

Es sorprendente la cantidad de información de alta calidad que se ofrece en las convocatorias de licitaciones. A veces esta información está disponible para su descarga anónima en los 'perfiles del contratante' de las webs de las entidades. En otras ocasiones, no es posible acceder a la información sin un registro previo (lo cual, en realidad, tampoco supone per se una gran dificultad para un atacante, aunque algo es algo). Sin embargo, incluso en los casos en los que no es posible descargar la información directamente ha sido posible acceder a ella por encontrarse alojada en otros sitios. A estos efectos, cabe recordar que el sector público no está constituido únicamente por Administraciones Públicas sino por centenares de empresas y otros entes que gestionan, de forma total o mediante fórmulas de colaboración público-privada, servicios esenciales. Por ejemplo, hemos localizado en un pliego (de cláusulas administrativas, paradójicamente) una descripción exhaustiva, incluyendo planos, fotografías, mediciones con marcas y modelos, etc. el sistema de telemando de un sistema de estaciones remotas de uno de los mayores sistemas de abastecimiento de agua de nuestro país.

• Documentos de divulgación.

Es especialmente frecuente en muchos sectores, especialmente en aquellos con fuerte participación de empresas constructoras y obra civil, que los contratistas adjudicatarios publiquen artículos descriptivos de la infraestructura ejecutada en el momento de su puesta en servicio. Estos artículos suelen publicarse en revistas especializadas en el sector en cuestión, revistas gratuitas que se financian a través de anunciantes. Estos anunciantes son las empresas proveedoras de equipos o subcontratistas especializados que han participado en la obra y que se anuncian justamente insertados en el texto descriptivo de la infraestructura en cuestión. Ello permite conocer no sólo el proceso o la distribución de las instalaciones (frecuentemente con fotografías) sino también tecnologías, marcas, modelos, etc.

• Artículos técnicos y similares.

Un subconjunto de dentro de esta categoría lo constituyen los artículos técnicos publicados por empleados de la compañía o Administración dando cuenta de algún caso especialmente relevante por su dificultad, carácter novedoso o relevancia de la infraestructura. Nos ha sido posible encontrar, por ejemplo, una ponencia presentada en un congreso dedicado a la ingeniería eléctrica la descripción de una subestación piloto construida en España en la cual se presenta un esquema con la arquitectura de la red de control y comunicación.

En otros casos se publican documentos destinados a destacar la buena gestión realizada con el fin de mejorar la imagen por la compañía. Hemos encontrado documentos donde se describe la red de control de la contaminación atmosférica de una I.C. dando todo tipo de detalles acerca de la red de estaciones de control sin considerar que estas instalaciones remotas constituyen puntos de acceso al sistema de control.

• Casos de éxito de proveedores.

Este punto es especialmente importante. Es extremadamente habitual que los contratistas que trabajan para una I.C., bien sea en la fase de construcción o en la explotación y mantenimiento, elaboren casos de éxito describiendo el tipo de servicio prestado, instalación ejecutada, implementación realizada, etc. En muchas ocasiones con la aquiescencia y en otros ante el desconocimiento del titular.

4.2 Origen

Nuestra investigación pone de manifiesto que la información es elaborada y publicada por todos los actores participantes en la vida de una II.CC. El papel de terceros tales como empresas constructoras o contratistas de mantenimiento es poco sorprendente. Sí lo es, en cambio, el hecho de las propias AA.PP. o empresas operadoras de II.CC. ofrezcan tanta información y con tanto detalle acerca de sus propias instalaciones. Una mención específica merecen ciertas universidades que se constituyen en auténticos repositorios online de información técnica muy específica.

En ocasiones los propios empleados ofrecen información fuera de la actividad diaria de la compañía; es el caso de los artículos técnicos publicados con el conocimiento (o no) de sus organizaciones. Hemos localizado, por ejemplo presentaciones elaboradas por personal de una I.C. para su empleo durante un curso de formación. El material describe exhaustivamente componentes y sistemas de la I.C. ofreciendo, incluso, detalles de la operación, gestión, etc., todo ello con abundante material gráfico.

4.3 Valoración del impacto

La valoración del impacto se basa en nuestra percepción de lo útil que podría resultar para un atacante la información obtenida. A estos efectos, téngase en cuenta que en ningún caso la información obtenida mediante búsquedas en internet es suficiente para llevar a cabo un ataque exitoso. Simplemente constituye un primer paso imprescindible que ha de ser complementado con acciones en otros muchos ámbitos. Hay algunos aspectos que hemos considerado especialmente graves:

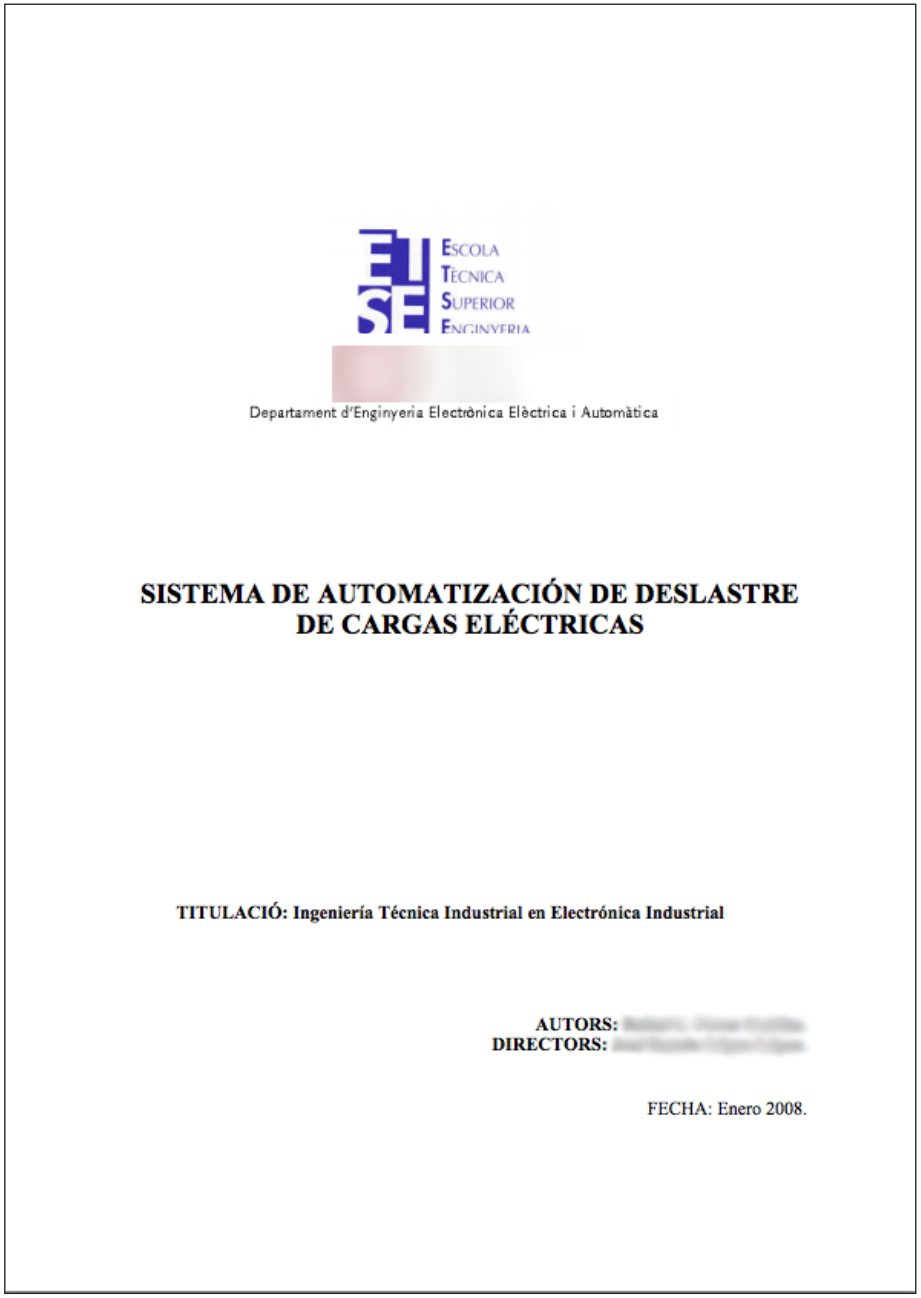
- La información relativa a infraestructuras, procesos y sistema de control.
- La información relativa a los sistemas de vigilancia y seguridad.

Recuérdese que la valoración realizada se refiere exclusivamente a la organización analizada. En un punto posterior trataremos de extrapolar los resultados para obtener una visión particular de cada sector.

Al observar la tabla resumen de resultados se observa que hemos considerado como de riesgo alto la información encontrada en tres sectores: química, agua y alimentación. Veamos cada uno de ellos:

INDUSTRIA QUÍMICA.

Hemos encontrado varios PFC con descripción exhaustiva de componentes
e instalaciones, incluyendo sus sistemas de control. Uno de ellos describe un sistema cuyo mal funcionamiento podría dejar fuera de servicio las instalaciones de una organización dentro del mayor polo químico de España. Todos los PFC se han realizado dentro de la misma universidad. El grado de detalle y la magnitud de las consecuencias de un ataque exitoso nos hacen juzgar el riesgo introducido como alto.



Escola Tècnica Superior Enginyeria

Departament d'Enginyeria Electrònica Elèctrica i Automàtica

SISTEMA DE AUTOMATIZACIÓN DE DESLASTRE DE CARGAS ELÉCTRICAS

TITULACIÓ: Ingeniería Técnica Industrial en Electrónica Industrial

AUTORS: [redacted]
DIRECTORS: [redacted]

FECHA: Enero 2008.

Portada de un proyecto fin de carrera

TRATAMIENTO Y DISTRIBUCIÓN DE AGUA POTABLE.

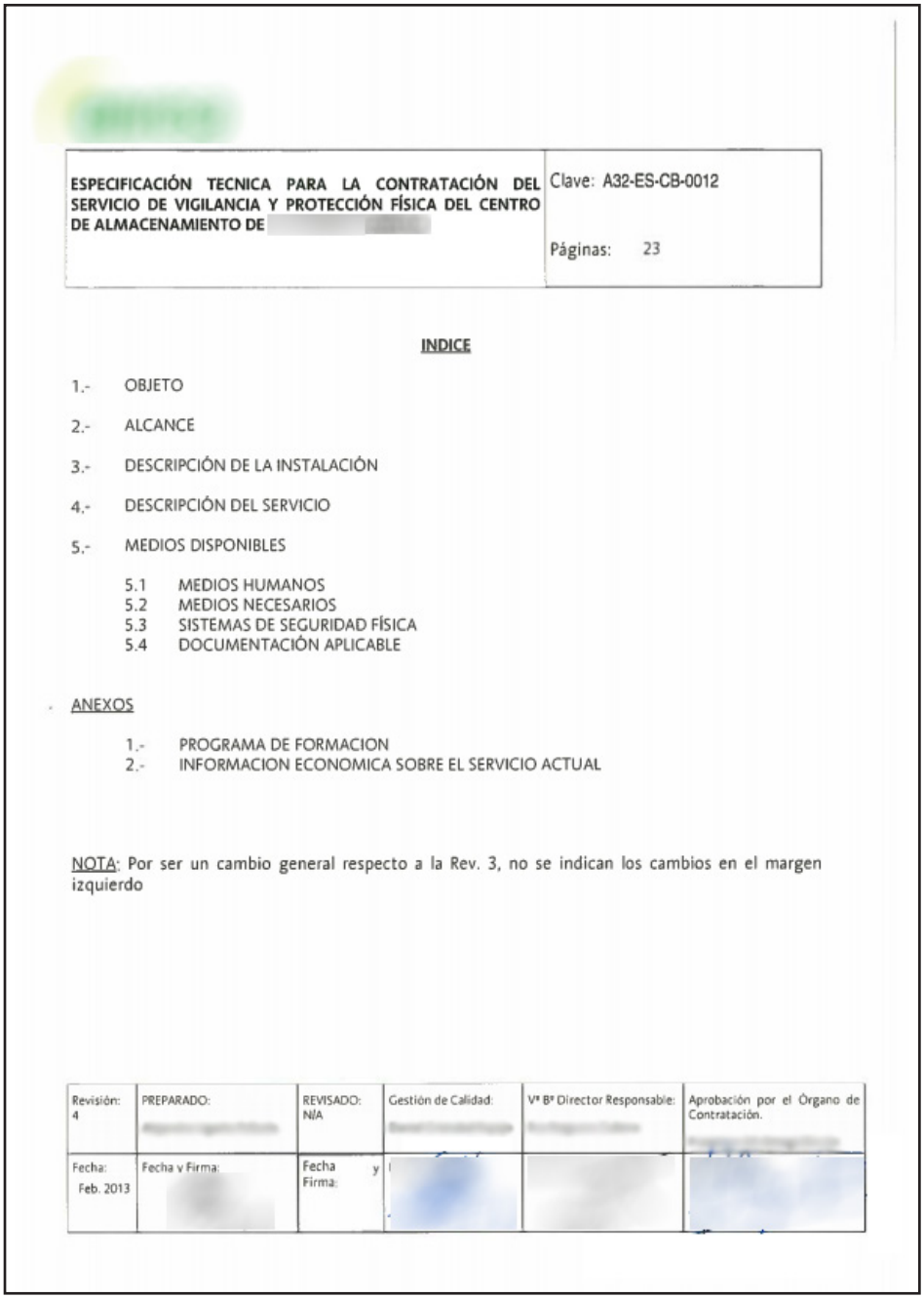
Se ha localizado información detallada acerca del sistema de control y comunicación con estaciones remotas, información contenida en el Pliego de Cláusulas Administrativas (algo verdaderamente extraño, ya que este tipo de información se suele proporcionar en los Pliegos de Prescripciones Técnicas Particulares e, incluso aquí, como un anexo). En particular se ofrecen fotografías de los cuadros de telemando, esquemas eléctricos y de la arquitectura de comunicación, relaciones de equipos con indicación de marcas y modelos, referencias de las empresas mantenedoras. Curiosamente, el perfil del contratante impide acceder a la información de los procesos sin registro previo. Sin embargo, la información está accesible mediante buscadores. Este problema no es exclusivo de este caso, ya que lo hemos detectado en otros sectores y organizaciones.

ALIMENTACIÓN.

En este caso la información obtenida excede el ámbito de los sistemas de control industrial. Se han localizado multitud de Pliegos. Por ejemplo, uno de ellos corresponde al servicio de seguridad física privada, y entre la información facilitada está la descripción del personal que compone los turnos, las tareas que deben realizar (rondas, recorridos, etc.). En otros Pliegos se facilita información sobre el control de acceso al recinto, planos con las instalaciones de detección y extinción de incendios, etc. En el ámbito propiamente de los sistemas de control hemos encontrado un caso de éxito de un proveedor describiendo la renovación del sistema de frío industrial de toda una línea de producto. En este documento, además, se indica el tiempo máximo que puede estar el sistema fuera de servicio sin que los alimentos almacenados se deterioren irreversiblemente (20 minutos en un día caluroso). El tipo de información junto con el tamaño de la población servida confiere a este caso la consideración de grave.

Cabe, además, hacer mención a dos casos especiales: la industria nuclear y el transporte.

Hablemos en primer lugar del caso nuclear. A pesar de que este sector es bastante reducido (en número de instalaciones y participantes) y de que, a priori, es considerado como crítico mucho antes de que se definiese como tal en el contexto actual, se ha localizado un documento que consideramos especialmente sensible. Se trata de un Pliego de un concurso de seguridad privada de una instalación en el que, además de describir el servicio, se ofrece una relación de las personas que actualmente desempeñan funciones de vigilancia en el recinto. Los nombres se relacionan mediante las iniciales de nombre y apellidos y, a continuación, se indica la población de residencia (todas de reducido número de habitantes por tratarse de un entorno rural) y el salario percibido. A todo esto hay que añadir que no es difícil encontrar en internet planos de las instalaciones, nuevamente en proyectos de fin de carrera y en documentos generados por la propia organización.



ESPECIFICACIÓN TECNICA PARA LA CONTRATACIÓN DEL SERVICIO DE VIGILANCIA Y PROTECCIÓN FÍSICA DEL CENTRO DE ALMACENAMIENTO DE	Clave: A32-ES-CB-0012 Páginas: 23

INDICE

NOTA: Por ser un cambio general respecto a la Rev. 3, no se indican los cambios en el margen izquierdo

Revisión: 4	PREPARADO:	REVISADO: N/A	Gestión de Calidad:	Vº Bº Director Responsable:	Aprobación por el Órgano de Contratación.
Fecha: Feb. 2013	Fecha y Firma:	Fecha y Firma:			

Ejemplo de Pliego de contratación de un servicio de seguridad privada

El segundo caso es del transporte. Este sector se considera uno de los primeros blancos en un ataque destinado a paralizar una ciudad o país y así es percibido por la población en general (las huelgas generales sirven perfectamente como demostración de esto). Y sin embargo, es posible localizar un curso de gestor de puesto de mando donde se describe exhaustivamente las instalaciones y operación de una de las mayores infraestructuras de transporte de España con multitud de material gráfico. Por añadidura, este material es ofrecido por un empleado de la compañía en el marco de un curso técnico impartido al margen de su organización (aunque imaginamos que con su conocimiento).

Por último, trataremos un sector con características especiales: la Administración (en sentido amplio). Decimos que es especial por dos razones:

- La adquisición de bienes y servicios del sector público debe realizarse de conformidad con ciertos criterios prefijados de publicidad y libre concurrencia.
- La Administración presta directamente multitud de servicios esenciales para los ciudadanos y muchos otros por mediación de contratas externas.

Para la investigación de este sector se ha elegido como objetivo el ayuntamiento de una de las mayores ciudades de España. Como cabía imaginar, los pliegos de concursos son el principal mecanismo por el cual se ofrece información de forma libre en Internet. Se han localizado multitud de estos documentos, algunos de los cuales describen con bastante detalle sistemas como circuitos de cámaras de televisión instalados en las calles, con planos, marcas y modelos, versiones de firmware, trazado de líneas de fibra óptica, etc. Lo mismo en relación con sistemas de control y regulación de tráfico. También hay documentos que describen salas de control, CPD, redes de comunicación, parques de equipos informáticos, sistemas de alumbrado público, sistemas de galerías subterráneas, etc. En muchos casos se ofrecen planos, tanto de centros específicos como de ubicación de elementos sensibles en las calles.

Es cierto que la mayor parte de esta información no ofrece posibilidades inmediatas de explotación. Sin embargo, las descripciones de sistemas, redes, servicios, etc. son de gran utilidad a la hora de establecer un marco general en el que encajar la información obtenida por otras fuentes o, incluso, diseñar búsquedas más detalladas o preparar un ataque de ingeniería social. Igualmente, se considera preocupante el grado de conocimiento de los procedimientos de actuación, tiempos de respuesta, servicios considerados críticos y demás que puede obtenerse del análisis de esta documentación. Por esta razón le hemos asignado un nivel de criticidad medio.

4.4 Percepción de la situación por sectores

Como ya hemos indicado, nuestro planteamiento ha consistido en seleccionar una organización destacada dentro de cada uno de los sectores considerados estratégicos para, a continuación, tratar de localizar información sensible para la seguridad de la misma, especialmente en lo relativo a ciberseguridad.

A pesar de restringir la búsqueda a una sola organización es inevitable localizar información relativa a otros integrantes del sector. Lejos de constituir una fuente de ruido, este hecho nos permite obtener una imagen más general acerca de la disponibilidad de información en el sector, lo que a su vez constituye el reflejo de toda una cultura profesional.

De este modo hemos podido establecer un criterio adicional que califica nuestra percepción subjetiva acerca de lo fácil o difícil que resulta localizar información en cada sector. Como podría pensarse, existe una correlación entre la facilidad de encontrar documentos sensibles y la gravedad de estos. No hay sorpresa en esto: la facilidad de encontrar cosas coincide con la probabilidad de que entre éstas haya algo sensible.
Esto parece reflejar la mentalidad imperante entre cada grupo de profesionales: si no se concibe la forma en que la información ofrecida pueda suponer un riesgo, no se imponen políticas de control de la misma.

De nuevo los sectores 'estrella' resultan ser los de Aguas, industria química y alimentación. A efectos de calibración de nuestra aproximación cabe decir que se localizó una licitación en la que se ofrecía información técnica extremadamente detallada a acerca de la red de distribución de agua potable en alta presión, incluyendo un mapa de la red con todos sus elementos, documentos descriptivos del sistema SCADA (con capturas de pantalla, lógica de desarrollo, marcas, modelos, etc.), un listado de coordenadas UTM de los elementos de la red (bombeos, plantas de tratamiento, depósitos…). Esta infraestructura no era objeto de escrutinio por nuestra parte y, precisamente por eso, nos permite confirmar nuestra impresión sobre el sector.

En el extremo opuesto se encuentra el sector aeroespacial, del que no ha conseguido localizarse ningún documento sensible.

Como ya se ha anticipado en el punto anterior, el conjunto de Administraciones públicas genera un importante volumen de documentación, especialmente a través de los pliegos de contratación de bienes y servicios, que suelen contener en los PPTP (Pliegos de Prescripciones Técnicas Particulares) información de detalle acerca de sistemas e instalaciones.

Por último, cabe hacer otra mención aparte al sector energético, especialmente proclive a proporcionar información en el ámbito académico en la forma de PFC, tesis y artículos de carácter científico-técnico.

4.5 Evaluación del riesgo

Para la evaluación del riesgo en cada sector se ha seguido el enfoque tradicional. Hemos empleado como impacto la criticidad de la información hallada, valor consignado en la tabla 1. Se ha asignado el siguiente valor numérico:

- Impacto bajo: 1
- Impacto medio: 2
- Impacto alto: 3

Del mismo modo, la probabilidad de que la amenaza se materialice se ha identificado con la facilidad de encontrar información pública en el sector en cuestión, según la misma tabla:

- Difícil: 1
- Medio: 2
- Fácil: 3

El producto de ambas variables proporciona el valor calculado del riesgo de causar daño a una organización a partir de la información sobre la misma hallada en internet.

Adicionalmente se ha evaluado otra variable, que hemos llamado magnitud del problema. Esta variable tiene en cuenta la dimensión de cada uno de los sectores en el contexto español, de forma que se emplea ésta como factor de ponderación para comparar unas organizaciones con otras. Podría pensarse en utilizar parámetros relacionados con facturación, volumen de ventas, producción, etc. Sin embargo, ese enfoque no es, en nuestra opinión, el correcto, por dos razones:

1.Hay sectores en los que es difícil evaluar esas magnitudes económicas (por ejemplo, la sanidad)

2.Hay sectores en los que la criticidad no está relacionada directamente con magnitudes económicas, de forma que su impacto en la sociedad es desproporcionadamente elevado en comparación con ese tipo de variables

Además, existe una consideración adicional. En lo relativo a la disponibilidad de información, el factor definitivo detrás del problema son las personas: esto es, la solución pasa por modificar la forma en que las personas gestionan la información dentro de cada organización. De esta forma, es más fácil que se filtren documentos sensibles cuanto mayor sea el número de personas que intervengan en su custodia, clasificación o difusión.

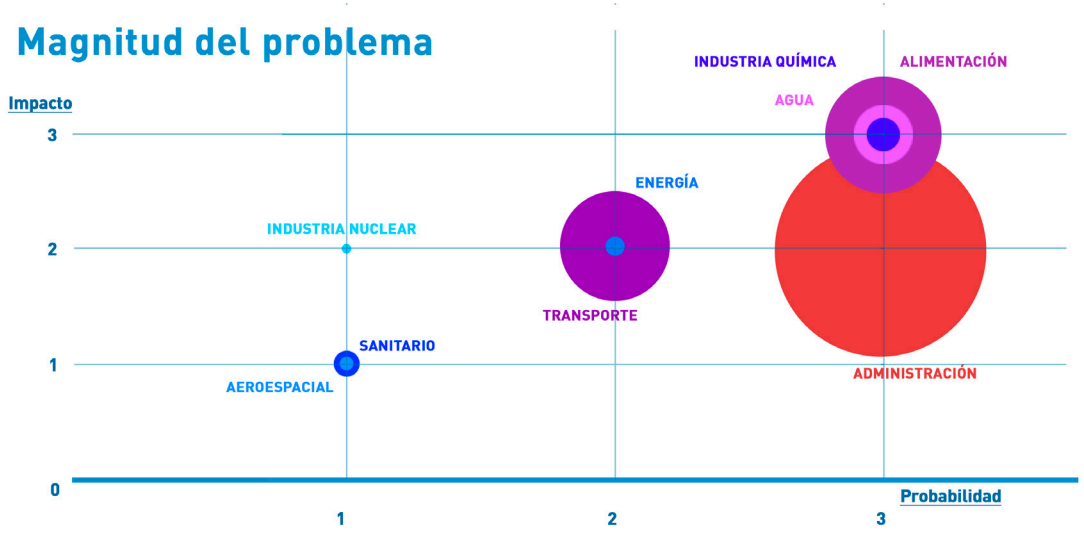
Por tanto, se ha optado por evaluar la magnitud del problema a partir del número de empleados en cada sector, utilizando datos proporcionados por el INE y referidos, cuando ha sido posible, al año 2012. Estos datos de ocupación se han normalizado en tanto por uno de total de empleados en el conjunto de los sectores críticos. De esta forma, la formulación es:

Magnitud del problema = Impacto x Probabilidad x Tamaño del sector

La tabla de evaluación de la ocupación es:

SECTOR	ÍNDICE TAMAÑO RELATIVO
Sanitario	0,18
Energía	0,02
Transporte	0,27
industria química	0,03
Industria nuclear	0,00
Agua	0,04
Alimentación	0,12
Administración	0,33
Aeroespacial	0,01

La siguiente gráfica recoge los resultados de los cálculos realizados. En eje de abcisas se representa la probabilidad asignada, en el de ordenadas se representa el impacto en cada sector mientras que el tamaño de los círculos es proporcional a la variable magnitud del problema.



El gráfico permite extraer algunas interesantes conclusiones:

• Los sectores con un menor número de empleados, como el aeroespacial o la industria nuclear, no suponen un grave problema a pesar de las ideas a priori acerca del impacto de un ataque sobre estas infraestructuras. Un tamaño pequeño del sector significa que una situación de riesgo (en cuanto a la gestión de la información) es abordable de forma manejable, dado el reducido número de personas implicado (lo que facilita la labor de cambiar procedimientos, establecer políticas, avanzar en la concienciación, etc.)

• Los sectores de agua, industria química y alimentación se encuentran en la zona alta tanto en cuanto a riesgo como a magnitud del problema, entre otras cosas a causa del elevado número de personas que trabajan en estas organizaciones.

• Algo similar ocurre con el transporte, que si bien no posee un valor de riesgo alto si se encuentra en una situación difícil debido a su tamaño.

• Se evidencia el grave problema que supone la gestión actual de la información en la Administración Pública y organizaciones afines. En el origen están los requerimientos de publicidad exigidos en los procedimientos de contratación.

En relación con este punto, hemos ampliado la investigación descubriendo, a modo de confirmación, que es posible localizar en internet información sensible publicada por los ayuntamientos de las tres mayores ciudades de España.

5 Conclusiones

5.1 Resultados de la investigación

El estudio realizado, si bien limitado por necesidad, pone de manifiesto un problema al que generalmente se concede poca o nula consideración cuando se habla de la ciberseguridad de sistemas de control industrial y su relación con la protección de infraestructuras críticas: la absoluta inconsciencia con la que se maneja y hace pública información sensible de gran interés para posibles atacantes. Ello es especialmente grave en un contexto en el que el diseño de una APT tiene como un elemento esencial el conocimiento profundo de la organización objetivo, tanto para diseñar el malware como los mecanismos de infección (por ejemplo, la planificación de un ataque de ingeniería social).

El tipo de información y los mecanismos de publicación son diversos, pero hay uno que destaca sobre todos los demás: las licitaciones de concursos públicos. Confluyen en esto dos circunstancias:

1. Los procedimientos de licitación deben garantizar, como uno de sus principios rectores, la publicidad y la libertad de concurrencia. Así se recoge en la Ley de Contratos del Sector Público. La transposición de la normativa europea ha exigido que todos los organismos públicos deban disponer de perfiles de acceso para contratantes a través de los cuales se publican en Internet los concursos y se ofrece la documentación asociada a los mismos.

2. La falta de conciencia de los posibles usos de la información facilitada. Tradicionalmente, la información de carácter técnico se recogía personalmente en la propia Administración contratante. De ahí se pasó al formato digital en CD y, finalmente, a ofrecer la descarga directa. De esa forma, información técnica muy específica se abre camino hasta el público general sin un escrutinio previo.

El segundo mecanismo que se encuentra detrás de la proliferación de información sensible es la necesidad, a medias científica y a medias comercial, de mostrar las propias habilidades, de forma que se publicitan las propias referencias con todo tipo de detalles. Cuando se mira desde el punto de vista de la ciberseguridad, no deja de resultar chocante la cantidad de información detallada que se ofrece al público general, en ocasiones ante el desconocimiento del promotor o titular y en otros casos con la aquiescencia cuando no la propia participación del mismo.

De resultas de todo ello es posible encontrar multitud de información sensible circulando por Internet. Lo cual, por cierto, sólo es uno de los posibles mecanismos por los que se puede obtener información. Otro factor clave, no considerado en este estudio, proviene de otra exigencia legal que afecta a la construcción de una infraestructura: el trámite de información pública. Este proceso, ineludible, obliga a que durante un tiempo determinado cualquier ciudadano pueda conocer los detalles de un proyecto para alegar lo que estime oportuno. La fórmula habitual consiste en poner a disposición de los ciudadanos el proyecto completo de las obras para su consulta.

Los sectores más afectados por la proliferación de información sensible fácilmente accesible son, a juzgar por la investigación:

- Tratamiento y distribución de agua.
- Alimentación.
- Industria química.
- Administraciones públicas.

Por el contrario, ha sido difícil localizar documentación referente a los sectores sanitario y aeroespacial.

5.2 Los riesgos de la información pública

Una de las razones del escaso control de la información en organizaciones que, por otra parte, disponen de controles de seguridad físicos de gran importancia, es la falta de conocimiento de cómo esa información puede ser utilizada. Una tipología básica (no exhaustiva) de los riesgos introducidos tiene cuenta si permiten:

Revelar detalles acerca de la red de control u otros equipos: arquitectura, marcas, modelos, protocolos empleados.

Descubrir detalles de un proceso físico, a través de una descripción o de imágenes como, por ejemplo, capturas de pantalla de las interfaces gráficas del software de supervisión.

Revelar detalles acerca de las personas que trabajan o trabajaron en la I.C. en algún momento de la vida de ésta (diseño, construcción, mantenimiento, explotación, etc.)

Permitir familiarizarse con un espacio físico determinado (por ejemplo, una planta industrial, un edificio, una sala de control) a través de planos, fotografías, etc.

Conocer rutinas y procedimientos internos, reproducir formatos de albaranes, partes u otros formularios, etc.

Obtener información acerca del sistema de seguridad física: número de vigilantes en cada periodo horario, detalles acerca de las rondas, tipo de sistemas de control de acceso, etc.

Obtener información acerca del sistema de seguridad lógica: arquitecturas, ubicación de firewalls, IDS, IPS, marcas modelos, antivirus, etc.

Identificar elementos críticos del proceso.

Conocer los sistemas de detección y respuesta ante emergencias: procedimientos, planos de instalaciones, tiempos de respuesta, etc.

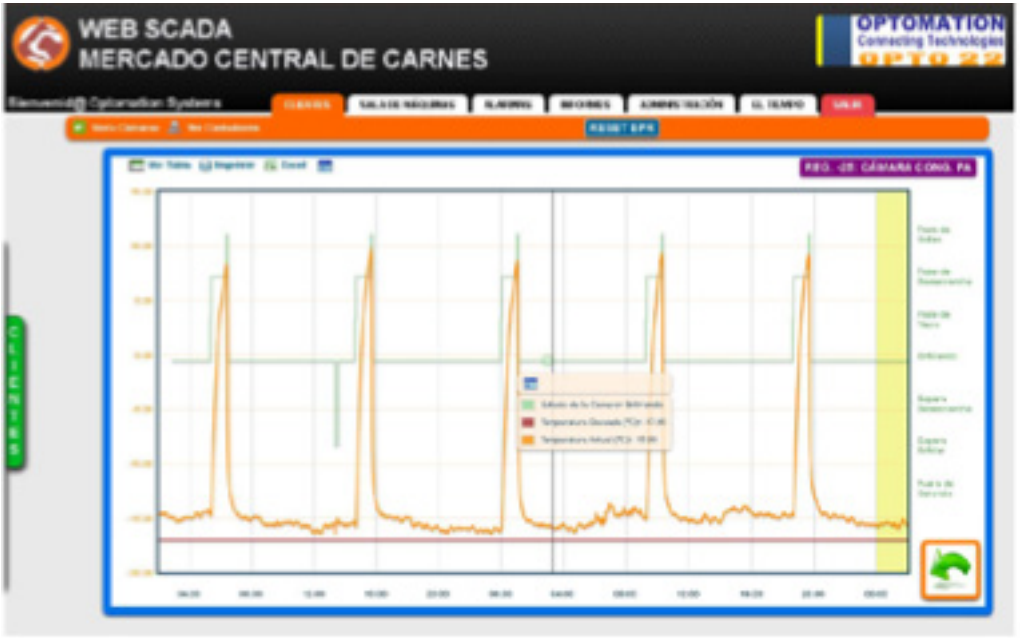
En nuestra investigación hemos encontrado información clasificable dentro de todas y cada una de las categorías anteriores. Y hay que tener en cuenta que, además, hay una última forma de explotar la información obtenida: diseñar ataques de ingeniería social combinando aspectos contenidos en los puntos anteriores. Esto es especialmente importante a la hora de planificar, por ejemplo, la forma de distribución de un malware diseñado para atacar a la organización.

5.3 A modo de ejemplo

Podemos ilustrar el riesgo de la información disponible públicamente mediante el siguiente experimento mental.

Si deseásemos atacar la I.C. del sector de la alimentación estudiada, ¿por dónde empezaríamos? A través del caso de éxito de un proveedor sabemos que se ha sustituido recientemente el sistema de control de la instalación frigorífica que mantiene en condiciones adecuadas cierto producto (destinado al abastecimiento de una ciudad, recuérdese). En ese mismo caso, además de marcas y modelos de componentes y protocolos de comunicación, se nos informa de algo importante: el sistema de frío no puede estar detenido más de veinte minutos en un día caluroso.

Gracias a la información obtenida de concursos públicos disponemos de planos de las instalaciones. También conocemos el sistema de control de accesos. De éste último nos interesa especialmente el método de control de entrada de vehículos, basado en el reconocimiento de matrículas. Localizamos una noticia en la que se explica cómo un usuario de la instalación consiguió burlar el sistema de control de forma habitual para evitar el pago de la tarifa establecida. Esta información la guardamos por si nos fuese necesario ganar acceso físico para hacer un reconocimiento in situ aunque, como veremos, no será necesario exponernos personalmente.



Captura de pantalla del software de supervisión ofrecido en el caso de éxito

A partir de ciertas debilidades conocidas diseñamos un malware dirigido a provocar la parada del sistema de frío a la vez que se inhibe la generación de alarmas. Sólo nos queda encontrar la forma de introducirlo en el sistema.

En el artículo técnico que nos sirvió de punto de partida el proveedor nos indica que dispone de capacidad de gestión remota de la instalación. Con una simple llamada telefónica averiguamos el nombre del técnico responsable y su correo electrónico. Nos es fácil dar detalles para ser creíbles gracias a la cantidad de detalles que conocemos de la infraestructura, todos ellos ofrecidos por personal relacionado con la misma en múltiples documentos.

Gracias a una red social de contactos profesionales averiguamos el nombre del jefe de mantenimiento de la I.C. Ahora enviamos un correo electrónico dirigido al técnico externo, al que le parecerá que ha sido enviado por un subordinado del jefe de mantenimiento (a fin de cuentas ya conocemos la estructura de los nombres de las cuentas de correo de la organización, por lo que nos es fácil simular una que no levante sospechas). Este correo contiene un software malicioso que se instala en su equipo. En el correo, además, se pide al técnico que se conecte al sistema central de producción de frío para verificar un posible problema. Para hacerlo verosímil se incluyen capturas de pantalla simuladas del SCADA elaboradas gracias a que conocemos su apariencia, que se muestra en los gráficos que ilustran el caso de éxito mencionado.

Cuando el técnico se conecta, nuestro software malicioso se instala en el servidor SCADA y espera el momento de actuar, típicamente una noche calurosa. En ese momento, se da orden de parada de todos los compresores de frío…

5.4 Líneas de acción

Para remediar la situación descrita en este informe se proponen una serie de iniciativas que agrupamos por categorías; su relación es la siguiente:

Iniciativas en el ámbito legislativo

- Modificar la ley para compatibilizar la publicidad y libre concurrencia con la necesidad de preservar cierta información.

- Modificar los procesos de información pública para excluir la información de detalle que pueda suponer un riesgo desde el punto de vista de la ciberseguridad.

Iniciativas en el seno del sector público

- Establecer limitaciones en los perfiles del contratante de las Administraciones públicas y otras organizaciones del sector público para impedir la descarga directa de información desde internet.
- Exigir confidencialidad a los participantes en los procesos de contratación.

Iniciativas en el seno de cualquier organización

- Realizar sesiones de concienciación en las organizaciones advirtiendo específicamente del riesgo que supone la disponibilidad pública de cierta información.
- Realizar búsquedas dirigidas para descubrir qué tipo de información sensible relativa a la propia organización es accesible desde internet.
- Exigir a los subcontratistas y proveedores confidencialidad en relación con los detalles de los trabajos, obras o servicios prestados.
- Establecer en las organizaciones políticas de clasificación de la información que dejen claro qué puede y qué no puede publicarse, y en qué condiciones.

Iniciativas en el ámbito científico-técnico

- Establecer limitaciones al contenido de PFC que puede hacerse público.
- Tener en cuenta al publicar artículos técnicos la difusión que éstos pueden tener fuera de los ámbitos a los que están dirigidos inicialmente.

5.5 Reflexión final

Cuando se habla de protección de II.CC. la atención suele dirigirse con gran facilidad hacia cuestiones técnicas o de procedimiento. El problema de la proliferación de información pública no suele ser tenido en cuenta, lo que es especialmente grave teniendo en cuenta que, en muchas ocasiones, es el propio personal de estas organizaciones el que se encuentra detrás de su difusión.

De nada sirven los esfuerzos realizados en otros ámbitos si no se avanza en el control de esta verdadera epidemia. Para ello, debe trabajarse en dos líneas diferenciadas: la concienciación de todo el personal relacionado con una I.C. (incluyendo a áreas como las administrativas que, si bien no tienen carácter técnico, sí pueden y de hecho publican información con un riesgo que no pueden calibrar) y la reforma de la legislación en materia de contratación en el sector público y los procedimientos de aprobación de proyectos de infraestructuras.

Y por último, cabe recordar que el factor humano es fundamental, como siempre ocurre en todo lo relativo a ciberseguridad. Las iniciativas de formación y concienciación deben incluir como punto fundamental el riesgo de la difusión incontrolada de información.

6 Referencias

[1] Ley 8/2011. Boletín Oficial del Estado, núm. 102, sec. I, pág. 43370. Abril de 2011.

[2] Resolución de 15 de noviembre de 2011 de la Secretaría de Estado de Seguridad. Boletín Oficial del Estado, núm. 282, sec. III, pág. 124147. Noviembre de 2011.

[3] Ley 30/2007 de 30 de octubre de Contratos del Sector Público.

[4] 1er Informe sobre la protección de infraestructuras críticas en España. 2011. S2 Grupo.

[5] 2º informe sobre la protección de infraestructuras críticas en España. 2012. S2 Grupo.

Sobre S2 Grupo

S2 Grupo es una empresa especializada en el desarrollo y prestación de productos y servicios relacionados con la ciberseguridad. Su objetivo es garantizar los procesos y proteger el activo más valioso de empresas y organismos públicos: la información.

Desde su creación, en 1999, S2 Grupo se ha convertido en una compañía referente en el entorno de la seguridad a nivel internacional. Entre sus clientes pueden encontrarse compañías líderes de los sectores de Distribución, Energía, Banca y Seguros, Sanidad, Industria y organismos de la Administración Pública.

La compañía tiene su sede en Madrid y su Centro de Servicios 24x7 se encuentra en Valencia. Además, cuenta con oficinas en Bogotá y México DF, S2 Grupo cerró 2013 con una facturación de 5,9 millones de euros, lo que supone un incremento del 18% con respecto a la cifra de negocio alcanzada un año antes. Las previsiones de facturación de S2 Grupo para el 2014 se sitúan en 6,25 millones de euros.

Este informe puede descargarse de la página web de S2 Grupo, **http://www.s2grupo.es**, o solicitándolo por correo electrónico a admin@securityartwork.es.

Madrid - Valencia - Bogotá - Ciudad de México

CYBERSECURITY LEADERSHIP
TO PROTECT THE WORLD

www.s2grupo.es