S2 GRUPO

Protección de Infraestructuras Críticas

Informe Técnico - Junio 2012

Sobre S2 Grupo

Fundada en 1999, es la primera empresa de la Comunidad Valenciana especializada en servicios globales de seguridad digital y una de las principales en el ámbito nacional.

Cuenta entre sus clientes con entidades de la importancia del Grupo Aviva, la Autoridad Portuaria de Valencia, Endesa, Hospitales Nisa, Red Eléctrica de España, la Universitat Jaume I de Castellón, Informática El Corte Inglés, Consum Cooperativa, la Universidad Politécnica de Valencia o Bankia, entre muchos otros.

La compañía cerró 2011 con unos ingresos de 4,4 millones de euros, lo que refleja un crecimiento del 39% respecto al ejercicio anterior, motivado por un aumento de la cartera de clientes y de la actividad de innovación. La inversión en I+D+i es uno de los ejes vertebradores de la compañía que en 2011 destinó 1,2 millones de euros a diferentes proyectos nacionales y europeos.

Autores
Pablo Marín
Antonio Villalón
Óscar Navarro

Diseño y maquetación
Karina Coste

Fecha de publicación
Junio 2012

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

S2 GRUPO

Ramiro de Maeztu 7, 46022 Valencia
T 963 11 03 00 # F 963 10 60 86

Orense 85, Ed. Lexington. 28020 Madrid
T 915 67 84 88 # F 915 71 42 44

Contenido

1. Introducción

Hace unos meses publicábamos

nuestro primer Informe sobre Protección de Infraestructuras Críticas ([3]), 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.

Queremos ahora complementar ese informe con un nuevo informe sobre la PIC en España, en este caso mucho más práctico y con un objetivo concreto:

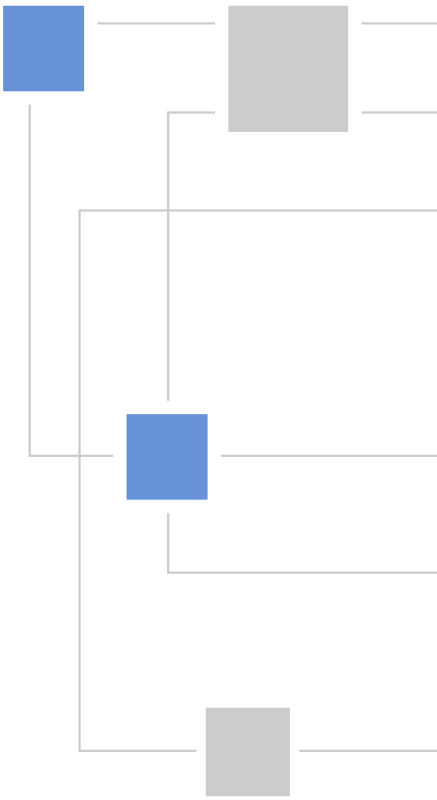
> ***Determinar si las infraestructuras críticas pueden considerarse "inseguras" en España (y si es posible, cuántas y de qué sectores) desde un punto de vista operativo.***

Para alcanzar este objetivo debemos en primer lugar determinar qué podemos entender por "inseguro"; en este caso, consideraremos inseguras aquellas infraestructuras que no hayan definido e implantado las medidas de seguridad que establece la Resolución de 15 de noviembre de 2011, de la Secretaría de Estado de Seguridad ([2]).

Esta resolución divide las medidas de seguridad en organizativas o de gestión, operacionales o procedimentales y de protección o técnicas; son estas últimas las que nos interesan, ya que desde el punto de vista normativo o procedimental la respuesta a nuestra pregunta únicamente la tendrá el CNPIC, en cuanto a operadores que no hayan realizado los planes correspondientes en cada caso, no dispongan de un análisis de riesgos correcto y completo o no hayan establecido procedimientos adecuados de seguridad, por poner unos ejemplos. Pero como esta información no nos la van a dar –obviamente– ni el CNPIC ni los propios operadores, al menos en términos generales, hay que buscar una alternativa: las medidas técnicas de seguridad.

Desde el punto de vista técnico diferenciamos las medidas de prevención y detección física y electrónica de las salvaguardas lógicas (así se establece en [2], aparte de la presencia de elementos de coordinación y monitorización fuera del ámbito del presente informe técnico).

Comprobar que desde el punto de vista físico una infraestructura crítica es o no segura implicaría reconocimientos y pruebas que difícilmente serían justificables para la elaboración de un informe como el presente, por lo que debemos ceñirnos en este caso a las medidas y elementos de seguridad lógica (cortafuegos, segregación de redes, aislamiento…) que se definen en la normativa.



Desde el punto de vista lógico, refinando la definición anterior de inseguridad: **¿qué entendemos por inseguro?** Para la realización de este informe consideraremos inseguro cualquier elemento accesible desde Internet –independientemente de su esquema de autenticación, si lo tiene– y que a priori, bajo nuestro criterio particular (que por supuesto será discutible) no deba estarlo.

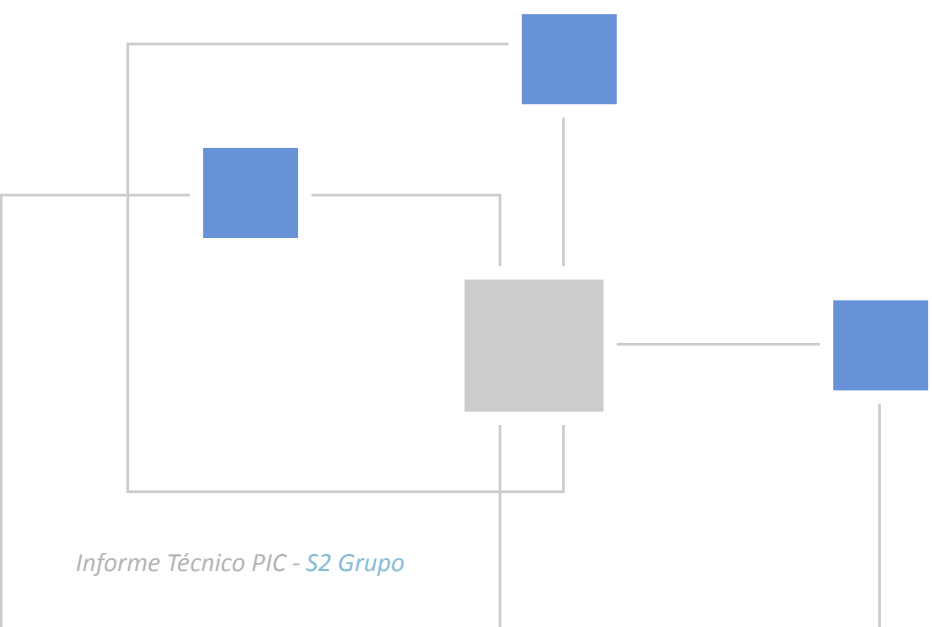
Dicho de otra forma: la página web de una organización debe estar disponible desde cualquier punto de Internet (otra cosa son las vulnerabilidades que introduzca, que obviamente para la realización de este informe no se consideran), pero no deben estarlo sus sistemas SCADA o los routers de comunicaciones troncales; por supuesto, existen elementos cuya accesibilidad desde la red es discutible (¿es necesario realmente el webmail?), pero llegar a este nivel de refinamiento sería imposible.

De esta forma, vamos a tratar de analizar de forma práctica elementos sensibles –o a priori sensibles– de sectores estratégicos que puedan introducir riesgos en infraestructuras críticas españolas mediante un análisis exclusivamente técnico de información públicamente disponible en Internet, sin llegar en ningún caso a pruebas que podrían considerarse hostiles (análisis de visibilidad, prueba de contraseñas por defecto…) contra esas mismas infraestructuras.

Es importante destacar en este punto que nuestro análisis no tiene, obviamente, ni fines estadísticos puros ni por supuesto debe considerarse completo, en el sentido de abarcar todas y cada una de las infraestructuras críticas españolas –cuyo catálogo, insistimos, es secreto–.

Simplemente hemos tratado de hacernos una idea de hasta qué punto, sin ejecutar pruebas hostiles ni lanzar ataques complejos contra nadie, podemos llegar a elementos de una infraestructura crítica nacional que pueden, potencialmente –y esto tampoco lo vamos a comprobar, por motivos obvios– introducir riesgos significativos; nada más.

Los resultados, bajo nuestro punto de vista, son claros: nos debe preocupar, y mucho, la seguridad lógica de las infraestructuras críticas; nos hemos encontrado situaciones que bajo nuestro punto de vista sólo son achacables a una falta de percepción del riesgo real (por diversos factores, pero resumidos en uno solo), y mientras que este problema de base no se resuelva, consideramos que en la seguridad de infraestructuras críticas queda mucho trabajo por hacer.



2. Planificación

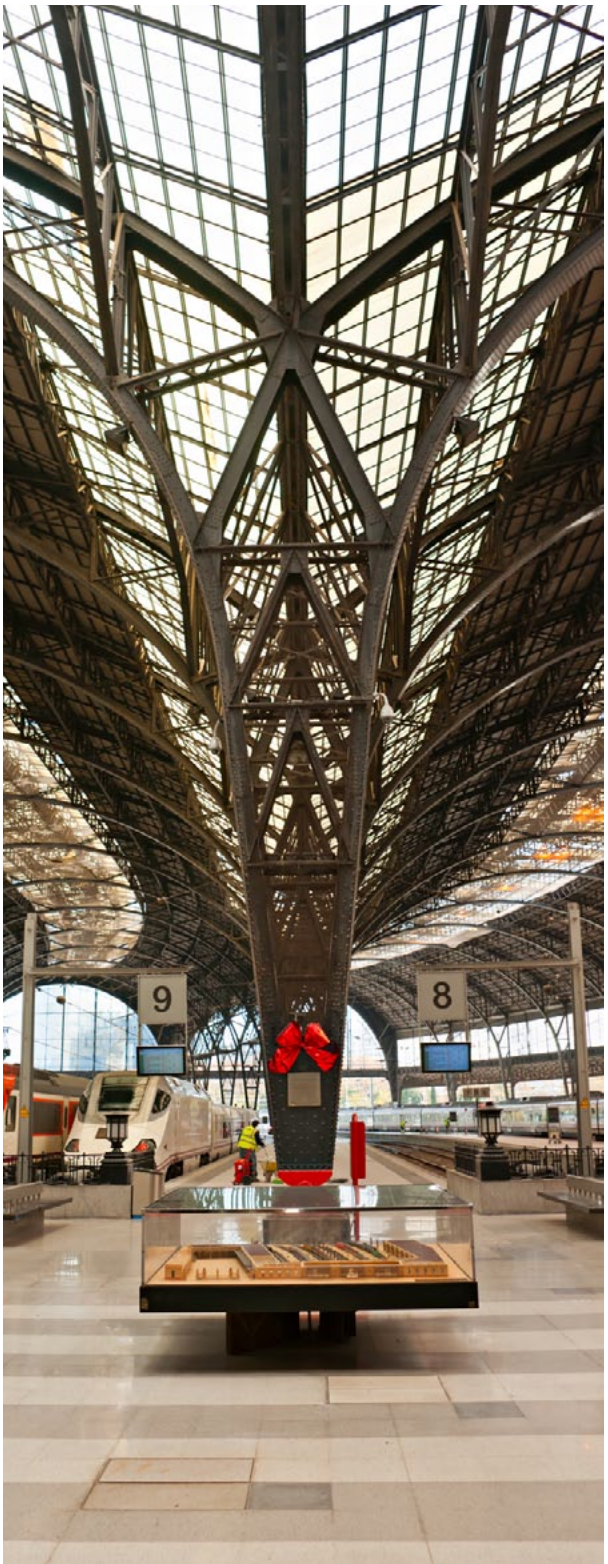
Para la ejecución de nuestro estudio hemos tratado de identificar elementos significativos asociados a infraestructuras críticas en España que puedan ser accesibles de una u otra forma –y por extensión, atacados– desde Internet; la Ley 8/2011 define en su anexo los sectores estratégicos españoles y los 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 de 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

De cada uno de estos sectores estratégicos queremos identificar elementos tecnológicos públicamente disponibles y que puedan introducir riesgos significativos en las infraestructuras críticas nacionales. Para ello definimos una serie de patrones (firmas) que nos permitan decidir, con una probabilidad alta y de forma automatizada si uno de estos elementos estará asociado a un sector o infraestructura particular. Estos patrones serán la entrada para el buscador SHODAN (http://www.shodanhq.com/), que nos dará los datos de elementos asociados a infraestructuras críticas en España, obteniendo una gran cantidad de resultados que se detallan a continuación y sobre los que se ha realizado el análisis correspondiente.

SHODAN es un motor de búsquedas que indexa los mensajes informativos, o "banners", que presentan los servidores conectados a Internet en puertos como el 80 (HTTP), el 23 (telnet), el 22 (SSH) o el 161 (SNMP), y permite llevar a cabo búsquedas avanzadas usando una variedad de filtros. Así, mientras que motores como Google o Bing permiten llevar a cabo búsquedas sobre el contenido de páginas web, SHODAN podría considerarse como un "buscador de máquinas", que además está disponible para cualquier usuario de Internet de forma gratuita.

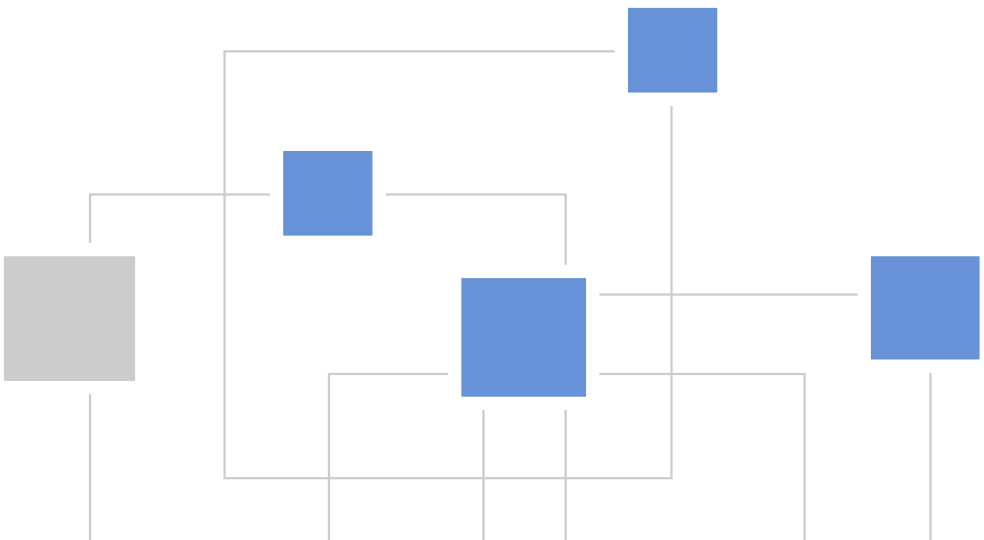
Aplicando búsquedas acerca de potenciales infraestructuras críticas, nos podemos hacer una idea de la información que podría llegar a conseguir un atacante sin ninguna infraestructura adicional; SHODAN es quizás uno de los buscadores más utilizado para obtener información relevante de posibles objetivos antes de un ataque directo.



Para definir el conjunto de firmas inicial con el que empezar la búsqueda –que como luego veremos será necesario refinar– vamos a identificar en primer lugar patrones que puedan representar un sector estratégico o una infraestructura crítica particular, bien por ser firmas genéricas de dicho sector (una firma como “ministerio” puede asociarse con una alta probabilidad al sector Administración mientras que una firma como “hospital” seguramente denotará el sector Salud) o bien por ser firmas asociadas a infraestructuras u operadores críticos (a pesar de que el catálogo es secreto, obviamente muchos de éstos son públicamente conocidos: grandes energéticas, bancos, gestores de infraestructuras de transporte, etc.).

Adicionalmente a los sectores estratégicos e infraestructuras y operadores críticos, un análisis de este tipo no podía excluir patrones de búsqueda relativos a sistemas de control industrial, los famosos SCADA, que cuando están desplegados en infraestructuras críticas y son públicamente disponibles a través de Internet introducen riesgos considerables en éstas, por encima de cualquier sector estratégico concreto. Para ello, hemos analizado los principales fabricantes, PLC, terminales táctiles, software de control… considerando que la información recabada a partir de estos datos podría constituir también un excelente punto de partida de cara a determinar cuántos de estos sistemas instalados en infraestructuras críticas son accesibles desde Internet.

En este sentido, el ICS-CERT ya había hecho una importante recopilación de estos productos –y por tanto de sus firmas–, recopilación que hemos tratado de complementar con datos provenientes de fuentes propias, mediante la identificación de un fabricante, elemento de control, etc., la determinación de sus sistemas (o incluso *releases* concretas) relacionados con SCADA y la identificación unívoca de las firmas asociadas a estos sistemas.



Por supuesto, no tenemos un mecanismo completamente fiable para determinar a ciencia cierta que un sistema de control está desplegado en una infraestructura crítica (cualquiera podría instalarse un sistema de control en su casa, aunque no sea lo habitual), pero con el conjunto de patrones ya tratado para eliminar falsos positivos, consideramos que los resultados obtenidos pueden asociarse a estas infraestructuras con una probabilidad alta.

Así, el conjunto de firmas, que conformará uno de los pilares para adquisición de datos, puede resumirse según la siguiente estructura:

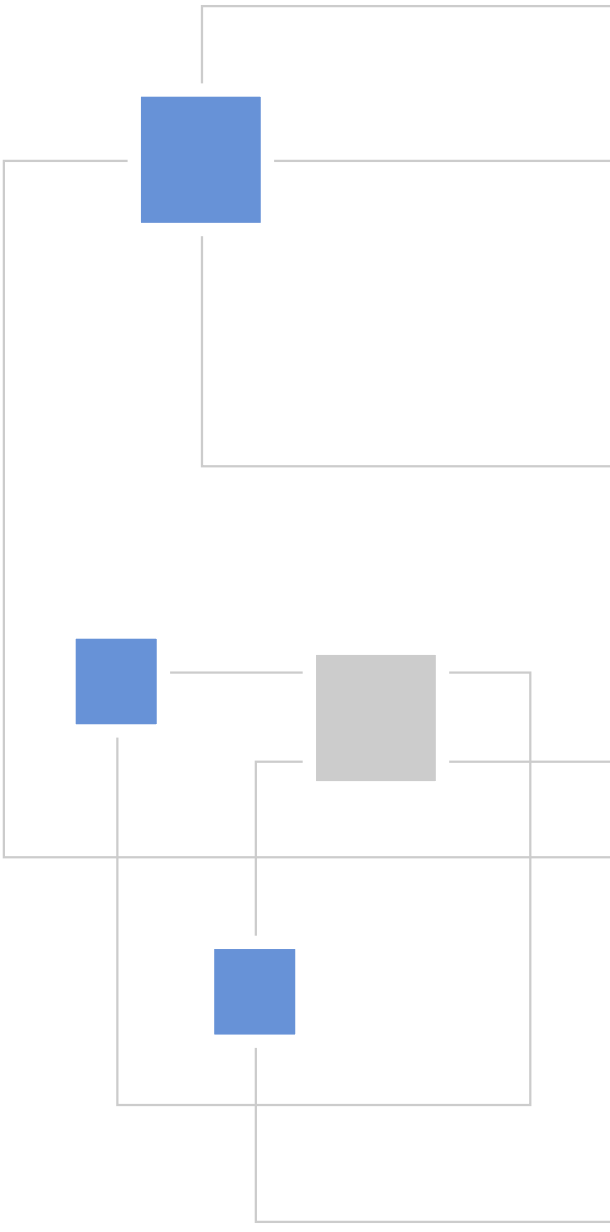
- **Firmas asociadas directamente a sectores estratégicos:**
  - Genéricas.
  - Asociadas a un operador de infraestructuras críticas.

- **Firmas asociadas a entornos SCADA:**
  - Genéricas.
  - Asociadas a productos de fabricantes de sistemas de control.

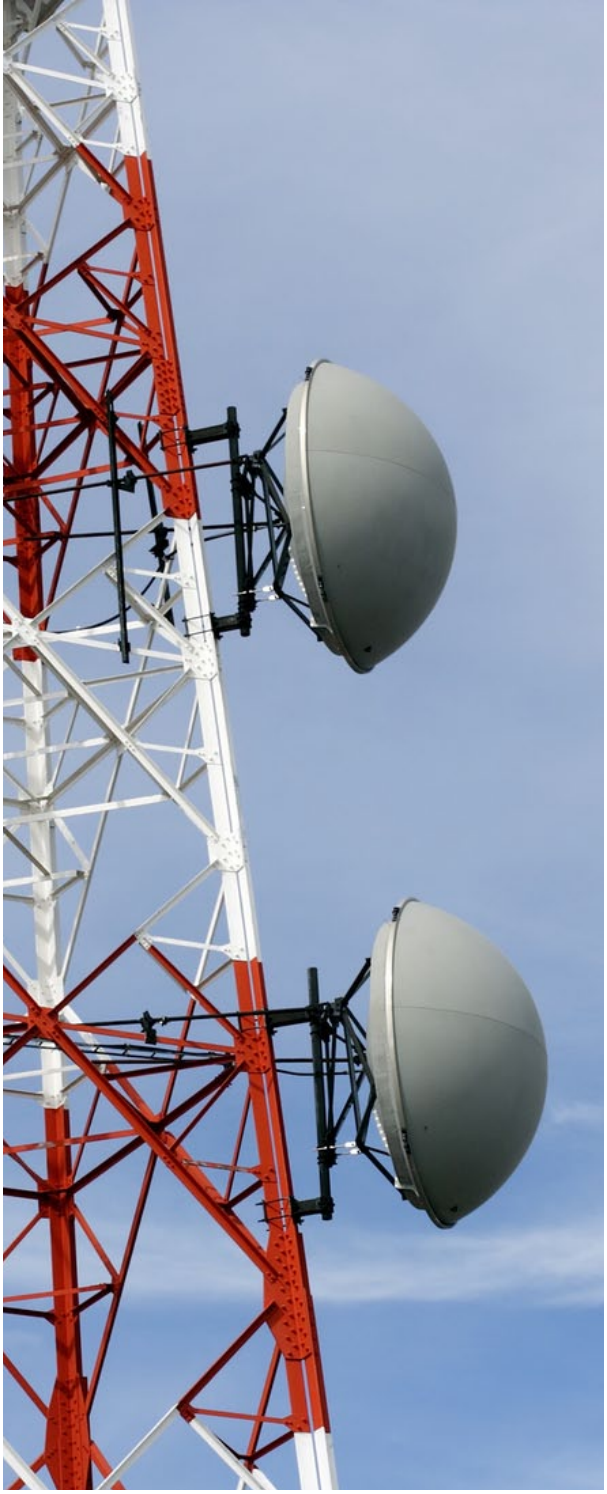
Adicionalmente a los patrones de búsqueda es interesante para nuestro análisis obtener resultados en función del direccionamiento público de grandes operadores críticos –como se ha indicado, el Catálogo es secreto pero algunos de estos operadores son de conocimiento general– y en función de la información whois de algunos rangos de red operados por terceros pero asociados a infraestructuras críticas –información que ya no proporciona directamente el buscador–. Los resultados obtenidos a partir de estas búsquedas en el direccionamiento son también una fuente interesante de datos que puede revelar posibles debilidades lógicas en infraestructuras críticas, por lo que se han tenido en cuenta en nuestro análisis siempre que técnicamente haya sido posible.

Los resultados obtenidos a partir de las entradas anteriores se han procesado e insertado en una base de datos que nos permita analizar la información y extraer conclusiones; algunas de ellas se muestran en el presente informe técnico, mientras que otros análisis de los datos recabados siguen en proceso y no serán publicados en abierto.

La información obtenida ha sido puesta a disposición de los actores correspondientes en cada caso para su explotación y diseminación dirigida, con el objetivo de que dichos datos se faciliten y sean de utilidad a los responsables de garantizar la seguridad en las infraestructuras críticas españolas.



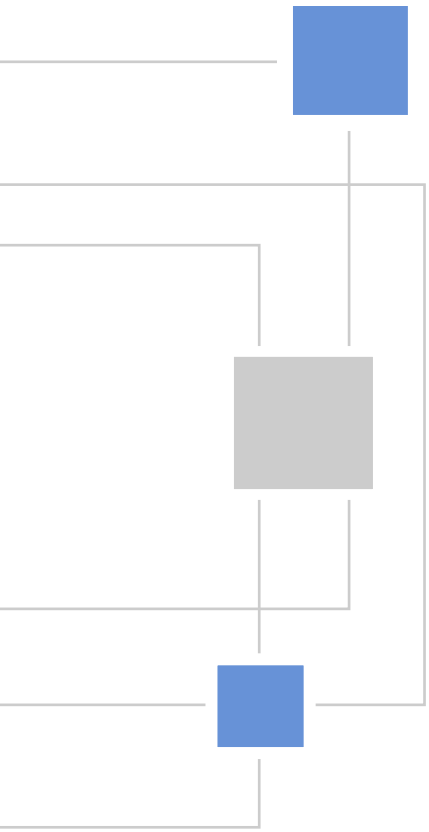
3. Adquisición de datos



Para cada una de las firmas identificadas como punto de partida se ha llevado a cabo una búsqueda en la página web del buscador SHODAN, limitando los resultados a los geolocalizados en España (modificador "*country:ES*"), y añadiendo los modificadores necesarios a la cadena de búsqueda para evitar los falsos positivos y cribar, en la medida de lo posible, los resultados que consideramos interesantes para el estudio. En ocasiones ha sido necesario concretar las firmas y en otras generalizarlas, tratando de que cada cadena final devuelva como máximo 100 resultados a priori interesantes. Esta eliminación de falsos positivos ha supuesto en algún caso una importante barrera en la adquisición de datos; si somos puristas, deberíamos haberla realizado en fases posteriores de nuestro trabajo, pero por motivos técnicos hemos hecho la criba durante la fase de adquisición.

Como indicábamos anteriormente, el *dataset* original que hemos utilizado para el análisis puede estructurarse en firmas asociadas directamente a sectores estratégicos (genéricas o correspondientes a un operador de infraestructuras críticas) y firmas asociadas a entornos SCADA (genéricas o asociadas a productos de fabricantes de sistemas de control).

En todos los casos ha sido necesario cribar manualmente elementos que, a pesar de incluir las firmas correspondientes a sectores estratégicos o entornos SCADA, no deben considerarse debilidades asociadas a infraestructuras críticas; por ejemplo, webs presenciales o transaccionales de pública disposición o sistemas de control más asociados a entornos domóticos que industriales.



Esta selección de firmas y modificadores de búsqueda y la automatización del proceso de adquisición han provocado que firmas en principio muy interesantes para nuestro análisis quedaran fuera de éste –quizás para una nueva versión de este informe técnico– debido al volumen de resultados generados y a la dificultad para determinar de forma automática si estábamos ante infraestructuras críticas reales o ante falsos positivos. Así, por ejemplo, grandes operadores de telecomunicaciones han generado muy pocos o ningún resultado en la fase de adquisición, lo cual puede llevarnos a una falsa sensación de seguridad pero que en realidad no significa más que la dificultad para separar el grano de la paja: pensemos simplemente en un *tag* identificativo de una gran operadora que está presente tanto en infraestructuras críticas como en sistemas ADSL domésticos.

Las listas completas de firmas finales, tras este proceso de filtrado inicial, correspondientes a las categorías definidas con anterioridad, no se presentan obviamente en este informe técnico; si alguien requiere esta información de forma justificada y desea solicitarla, puede ponerse en contacto con nosotros para analizar cada caso particular y remitir, si corresponde, la información estrictamente necesaria.

De forma adicional al conjunto de firmas, este equipo ha tratado de ampliar la búsqueda de elementos asociados a infraestructuras críticas mediante dos líneas de adquisición complementarias: la primera de ellas hace referencia a la información *whois* asociada a elementos de operadores críticos no gestionados directamente por ellos, pero sí operativos bajo su infraestructura de red.

Estos elementos no suelen tener un banner indexado por SHODAN que referencie al operador en cuestión, pero el rango de red en el que se ubica la dirección IP del elemento sí presenta en muchas ocasiones esta referencia; esta es la situación habitual de, por ejemplo, elementos de comunicaciones gestionados por el proveedor pero que prestan servicio en una infraestructura crítica. Así, para ampliar el *dataset* inicial se han seleccionado las grandes operadores de comunicaciones que prestan servicio en España y se han localizado elementos de comunicaciones operador por éstas pero con información *whois* asociada a una infraestructura u operador crítico (a partir del conjunto de firmas original que se utilizó para buscar en SHODAN).

La segunda línea de adquisición se basa en el rango de direccionamiento IP de grandes operadores críticos. Es sencillo, para los principales operadores de infraestructuras críticas (que recordemos forman parte del conjunto de firmas original), determinar alguno de los rangos de red que tienen reservados (una o más clases C) y en ese rango buscar servicios potencialmente peligrosos –insistimos, sin entrar en análisis hostiles–, por ejemplo puertos abiertos como el 23/tcp (TELNET) o el 22/tcp (SSH) utilizados para acceso de terminal remota y que en principio no deben ser accesibles directamente desde Internet. Esta búsqueda se ha realizado tanto a partir de SHODAN como mediante barridos horizontales.

Esta aproximación y la anterior nos han permitido ampliar ligeramente el volumen de resultados obtenidos de forma previa, así como asociar a operadores –y por extensión a sectores estratégicos– la información obtenida.

Para realizar el proceso de recolección de información se ha empleado el API de SHODAN para el lenguaje de programación Python. SHODAN limita las características y la cantidad de las búsquedas que pueden llevarse a cabo en función de la funcionalidad contratada, que se asocia a una *"API key"*. De cada firma hay que tener en cuenta el valor de la información que nos daría un positivo del patrón, así como el número de falsos positivos asociados a la firma y en definitiva la información útil que proporciona.

4. Procesamiento

4.1 Recopilación inicial de los datos

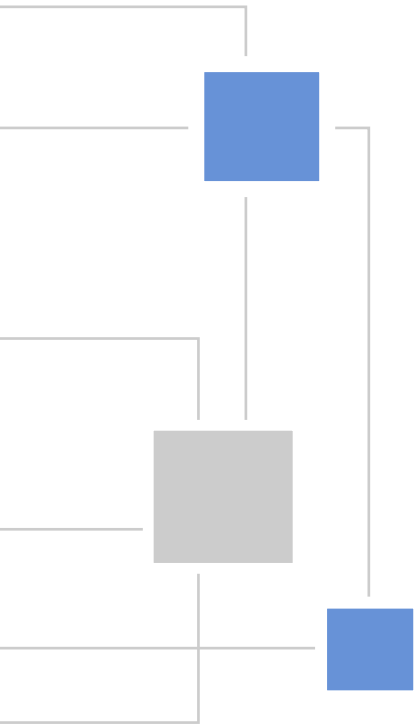
Inicialmente se ha llevado a cabo una búsqueda automática mediante el API para cada una de las firmas recopiladas, limitando los resultados a España y obteniendo un máximo de 100 entradas por consulta tal y como se ha indicado. No se ha limitado el ámbito temporal de las consultas, esto es, se han obtenido todos los datos disponibles en SHODAN, salvo por el límite en el número de los mismos.

Estos datos se han guardado en un prototipo de base de datos, implementada con SQLite, que servirá de soporte para la herramienta de análisis descrita posteriormente en el presente informe. En concreto, el esquema de la tabla donde se guardan los resultados devueltos por SHODAN es el siguiente:

```
CREATE TABLE entry(
        id INTEGER PRIMARY KEY AUTOINCREMENT,
        city TEXT,
        updated TEXT NOT NULL,
        ip TEXT NOT NULL,
        longitude REAL,
        country_name TEXT,
        hostnames TEXT,
        country_code TEXT,
        latitude REAL,
        data TEXT NOT NULL,
        port INTEGER NOT NULL,
        timestamp TEXT NOT NULL
);
```

4.2 Eliminación de falsos positivos

Para cada una de las familias de firmas identificadas previamente, a pesar de haber hecho una criba inicial que elimine las firmas que introducen ruido o falsos positivos en los resultados, se ha realizado una eliminación de falsos positivos automática así como manual.



En muchas de las firmas asociadas directamente a sectores estratégicos, tanto genéricas como especialmente en aquellas asociadas a un operador de infraestructuras críticas, ha sido necesario eliminar directamente resultados asociados a servicios como HTTP o HTTPS. Esto se ha realizado debido al volumen de información obtenida y al número de falsos positivos que podrían alterar significativamente los resultados del análisis sin posibilidad de automatizar su criba.

Además, según lo indicado previamente, del conjunto de firmas original se han eliminado entradas demasiado genéricas que introducían ruido en los resultados y elementos que de forma masiva están conectados a Internet, en nuestra opinión sin ningún tipo de justificación. No estimamos que dichos elementos, aun pudiéndose considerar asociados a infraestructuras críticas, introduzcan un nivel de riesgo significativo al menos, cada uno de ellos de forma individual. Un ejemplo de esta situación son impresoras conectadas a Internet, en especial en instalaciones asociadas a investigación.

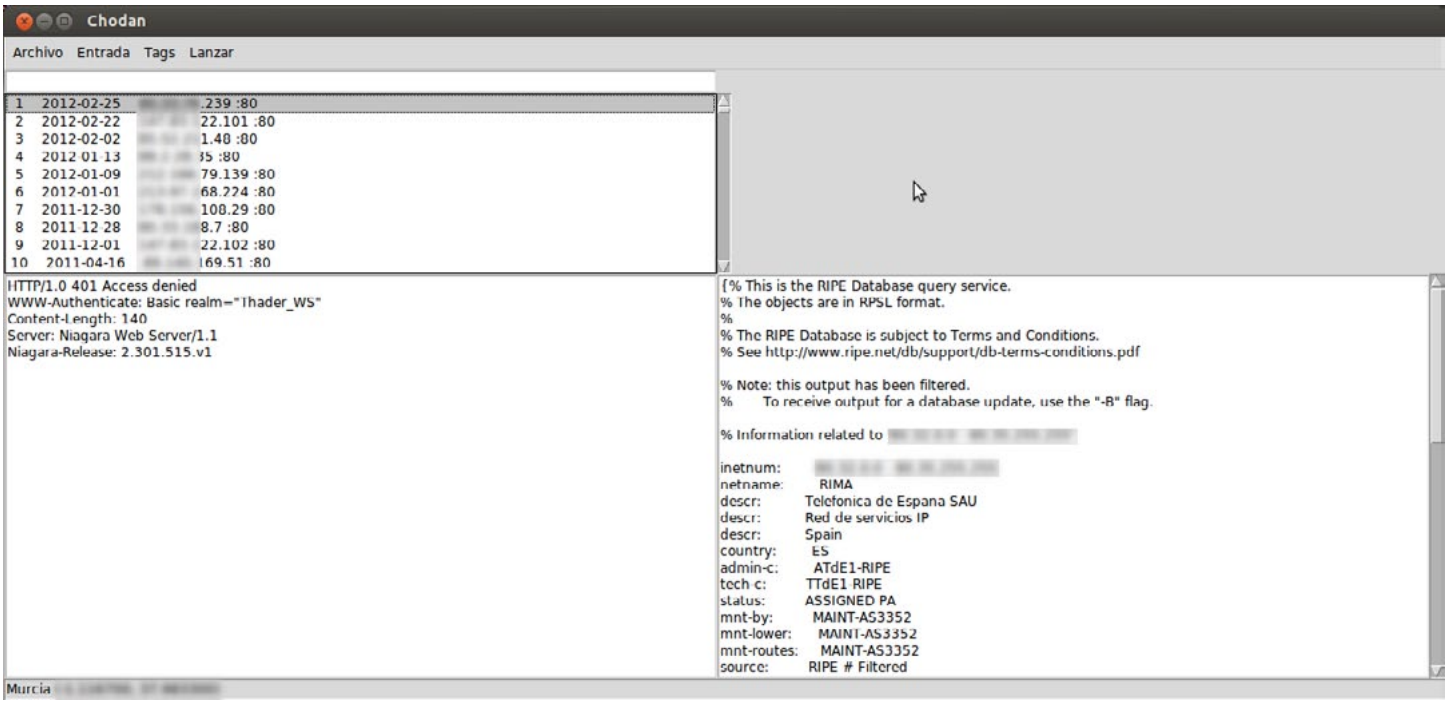
En el caso de los entornos SCADA y las firmas asociadas a éstos, el trabajo previo de determinación de firmas exactas ha posibilitado que el número de falsos positivos sea despreciable y no haya sido necesario un refinamiento adicional a los datos obtenidos previamente.

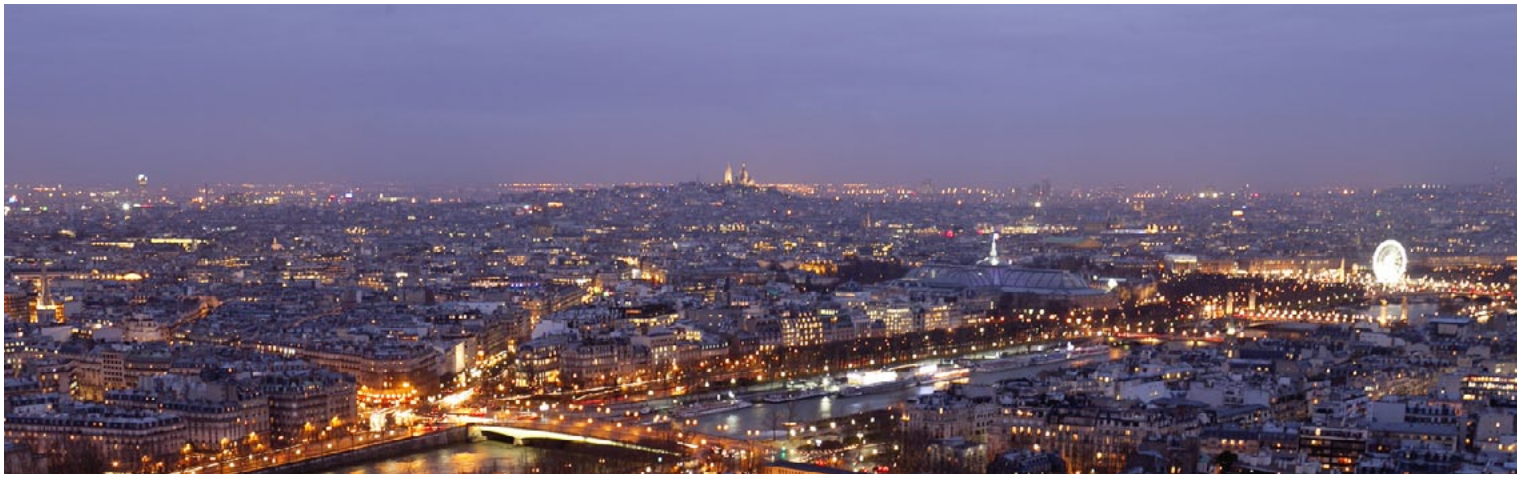
Para la búsqueda de elementos no basada directamente en firmas, tanto de datos *whois* como de rangos de red, la criba se ha realizado consultando directamente puertos que este equipo considera potenciales debilidades para cualquier infraestructura (crítica o no). Algunos ejemplos, sin ánimo de proporcionar una relación exhaustiva, son: 22 (SSH), 23 (TELNET), 161 (SNMP) y diferentes puertos asociados a motores de bases de datos, como MySQL o Microsoft SQL Server.

Por último, es necesario indicar que los resultados obtenidos por este equipo han estado sujetos a un análisis manual –al menos muestral–para identificar posibles falsos positivos que pudieran alterar resultados de forma significativa (por supuesto, no se ha bajado al detalle de cada uno de los resultados obtenidos).

4.3 Herramienta de análisis de datos

Se ha desarrollado el prototipo de una herramienta gráfica en Python, con la librería Tkinter, para facilitar el análisis de los datos recopilados.





Esta herramienta permite:

- Visualizar en una misma pantalla la lista de resultados de SHODAN disponibles en la base de datos, junto con el *banner*, el *whois* y la geolocalización de la entrada seleccionada en la lista.

- Clasificar los resultados mediante etiquetas o *tags*. Así, tras estudiar un resultado, se le puede asociar el *tag* "`visto`". Si por ejemplo se trata de un sistema SCADA, se le puede asociar el tag "`scada`", y si además es vulnerable, el *tag* "`vuln`".

- Llevar a cabo búsquedas a partir de las etiquetas y del contenido de los banners. Por ejemplo, se podría indicar la consulta "`-tag:visto siemens`", para buscar por resultados que contengan "`siemens`" en el *banner* y que no han sido vistos.

- Lanzar de forma automática herramientas contra las IP de los resultados; por ejemplo, abrir un navegador, ejecutar herramientas de escaneo de puertos, SNMP, etc.

El sistema de etiquetas se apoya en dos tablas adicionales en la base de datos:

```
CREATE TABLE tag(
      id INTEGER PRIMARY KEY AUTOINCREMENT,
      name TEXT NOT NULL,
      description TEXT
);
```

```
CREATE TABLE tag_entry(
      id INTEGER PRIMARY KEY AUTOINCREMENT,
      entry_id INTEGER NOT NULL,
      tag_id INTEGER NOT NULL,
      FOREIGN KEY(entry_id) REFERENCES entry(id),
      FOREIGN KEY(tag_id) REFERENCES tag(id)
);
```

Asimismo, otro script lleva a cabo en modo “offline” las consultas en la base de datos de *whois* e inserta la información en la tabla correspondiente, con los fines expuestos con anterioridad:

```
CREATE TABLE whois(
      id INTEGER PRIMARY KEY AUTOINCREMENT,
      ip TEXT NOT NULL,
      whois TEXT NOT NULL
);
```

4.4 Resultados

Se incluyen a continuación los resultados obtenidos para cada una de las firmas una vez se han eliminado falsos positivos, constituyendo un total de **1.180 resultados** a fecha de redacción del presente informe (94 correspondientes a sectores y 1.086 correspondientes a sistemas SCADA).

Sector estratégico	Firmas generales	Firmas particulares	TOTAL
Administraciones Públicas	38	0	38
Espacio	0	0	0
Industria nuclear	0	0	0
Industria química	1	7	8
Instalaciones de investigación	8	2	10
Gestión de aguas	5	2	7
Energía	15	6	21
Salud	4	0	4
TIC	0	0	0
Transporte	4	0	4
Alimentación	2	0	2
Sistema financiero y tributario	0	0	0
TOTAL	**77**	**17**	**94**

Fabricantes sistemas de control	Sistemas de control genérico	TOTAL
928	158	1.086

Para cada uno de los anteriores 1.180 resultados se ha obtenido la relación de entornos “vivos”, es decir, de aquellos que en la actualidad permanecen accesibles desde Internet. Para ello se ha automatizado la conexión a la dirección y puerto destino identificados por SHODAN, determinando que de los resultados anteriores, **907 siguen activos** a fecha de redacción del presente informe.

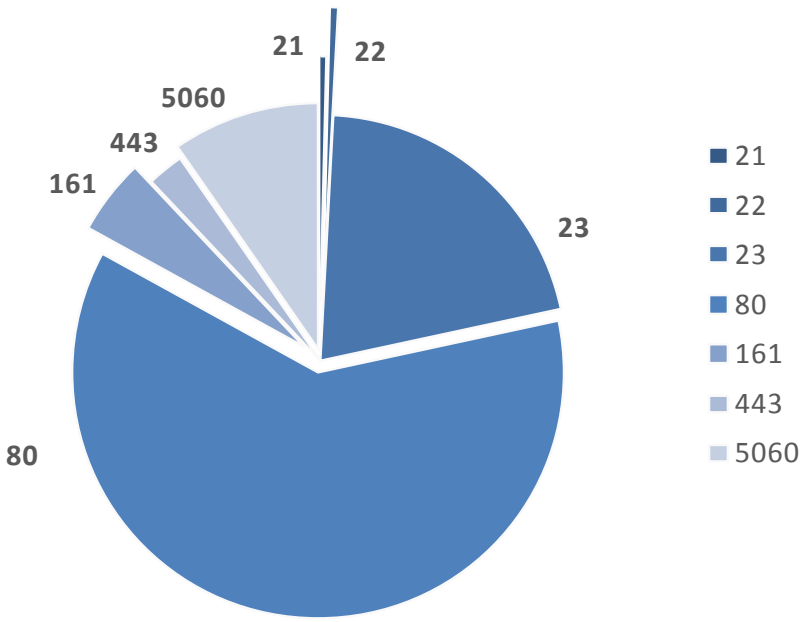
3. Análisis

La pregunta que nos planteábamos al inicio y a la que nuestro análisis trata de dar respuesta era: ¿cuántas –potenciales– infraestructuras críticas presentan algún modelo de acceso remoto no adecuado para su seguridad, y por tanto son susceptibles de ser atacadas directamente desde Internet? De entrada, todos los resultados obtenidos en las fases anteriores son significativos ya que se ha invertido un esfuerzo considerable en la eliminación de ruido y falsos positivos. Así, nos hemos encontrado **1.180 elementos** que de una u otra forma están asociados a infraestructuras críticas y que introducen, siempre bajo nuestro criterio –que no es matemático y puede ser discutible- debilidades o, directamente, vulnerabilidades relevantes en la infraestructura afectada.

Estos resultados, en crudo y procesados, así como los paquetes de firmas originales, han sido remitidos a los organismos competentes para cualesquiera acciones que éstos determinen a partir de los mismos.

5.1 Protocolos de acceso

A partir de los resultados obtenidos en la adquisición y procesamiento de datos, la distribución de protocolos de acceso a elementos asociados a infraestructuras críticas es la siguiente:



Distribución puertos abiertos

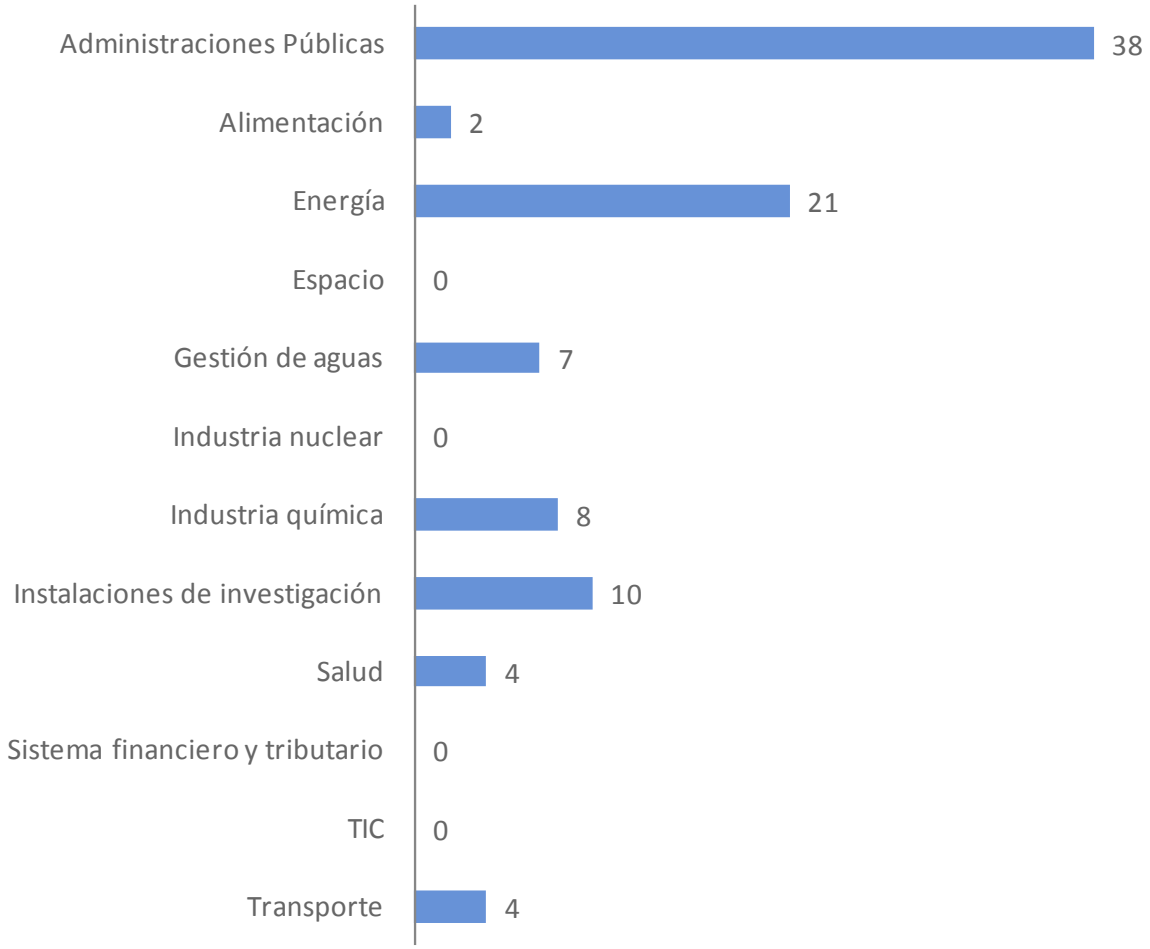
A la vista de los resultados, destaca el uso intensivo del protocolo HTTP (puerto 80) para acceso a elementos IT de infraestructuras críticas. Este protocolo no incorpora cifrado de datos, con lo que independientemente de su esquema de autenticación si lo tiene, no parece una buena aproximación para la seguridad corporativa de estas infraestructuras, como tampoco lo es el uso del protocolo TELNET (puerto 23), utilizado habitualmente para acceso de terminal remota –privilegiado o no– y que como el anterior transmite la información en texto claro entre emisor y receptor. De la relación de puertos anteriores, este equipo consideraría únicamente aceptable la disponibilidad del protocolo HTTPS (puerto 443), que cifra la información en tránsito y permite autenticar los extremos; en cualquier caso, hacemos hincapié en que acceder a un dispositivo de esta forma, directamente desde Internet, siempre introduce vulnerabilidades significativas y, en el caso de infraestructuras críticas, al que se ciñe este informe técnico, no debería estar permitido por la política de seguridad corporativa.

Adicionalmente, es especialmente relevante que muchos de los accesos a través de HTTP a sistemas de control de potenciales infraestructuras críticas ni siquiera presentan un esquema de autenticación básico; en concreto, este equipo ha detectado más de 100 entornos SCADA a los que ha sido posible acceder con un simple navegador sin ningún tipo de contraseña. Este hecho, aunque ya de forma residual, se extrapola al acceso TELNET: se han encontrado elementos accesibles a través de este protocolo que directamente ejecutaban un intérprete a la espera de recibir órdenes. Por supuesto, no hemos entrado a analizar en ningún caso los sistemas que puedan admitir unas credenciales por defecto, pero nuestra impresión es que su número sería también relevante, ya que aparentemente en ocasiones “se deja caer” el dispositivo en la red, con los niveles de seguridad que el fabricante haya querido aportar en cada caso.

Es también llamativa la presencia del protocolo SIP (puerto 5060) en infraestructuras críticas españolas. Este protocolo está asociado a servicios de VoIP, con lo que su presencia en el conjunto de datos adquirido indica la susceptibilidad de atacar estos sistemas de comunicaciones desde cualquier punto de Internet, interrumpiendo potencialmente la transmisión de voz en infraestructuras críticas. De la misma forma, el protocolo SNMP (puerto 161), utilizado para gestión remota de dispositivos, en opinión de este equipo, no debe estar accesible desde Internet bajo ningún concepto y sorprendentemente se han hallado elementos que permiten esta gestión –al menos la consulta de datos– a través de SNMP. Aunque de cualquier forma es preocupante, en el caso de que alguno de estos dispositivos tuviera instalada una *community* por defecto se podría acceder desde cualquier punto de Internet a muchísima información útil para ataques más duros o incluso, bajo ciertas circunstancias, modificar la configuración del dispositivo si la *community* permite escritura.

5.2 Sectores estratégicos

La distribución de hallazgos significativos por sector estratégico es la mostrada en la siguiente gráfica:



Hallazgos por sector

Para la elaboración de la gráfica anterior únicamente se han tomado como datos de entrada los asociados a la clasificación de las firmas por sector estratégico, no las correspondientes a elementos SCADA, debido a la imposibilidad de asociar de forma automatizada, en la mayor parte de casos, un elemento de control a un sector concreto.

Como podemos comprobar, es el sector relacionado con la Administración Pública el que presenta más elementos susceptibles de ataque desde Internet, seguido de la industria química y el sector energético. En el caso de las AAPP, la mayor parte de hallazgos corresponden a elementos de comunicación, aparentemente troncales, de diferentes administraciones (General del Estado y autonómica principalmente) que son accesibles desde Internet mediante autenticación pero sin cifrado; esta situación es considerada una debilidad, ya que este acceso debería estar habilitado únicamente desde aquellos entornos desde los que sea estrictamente necesario.

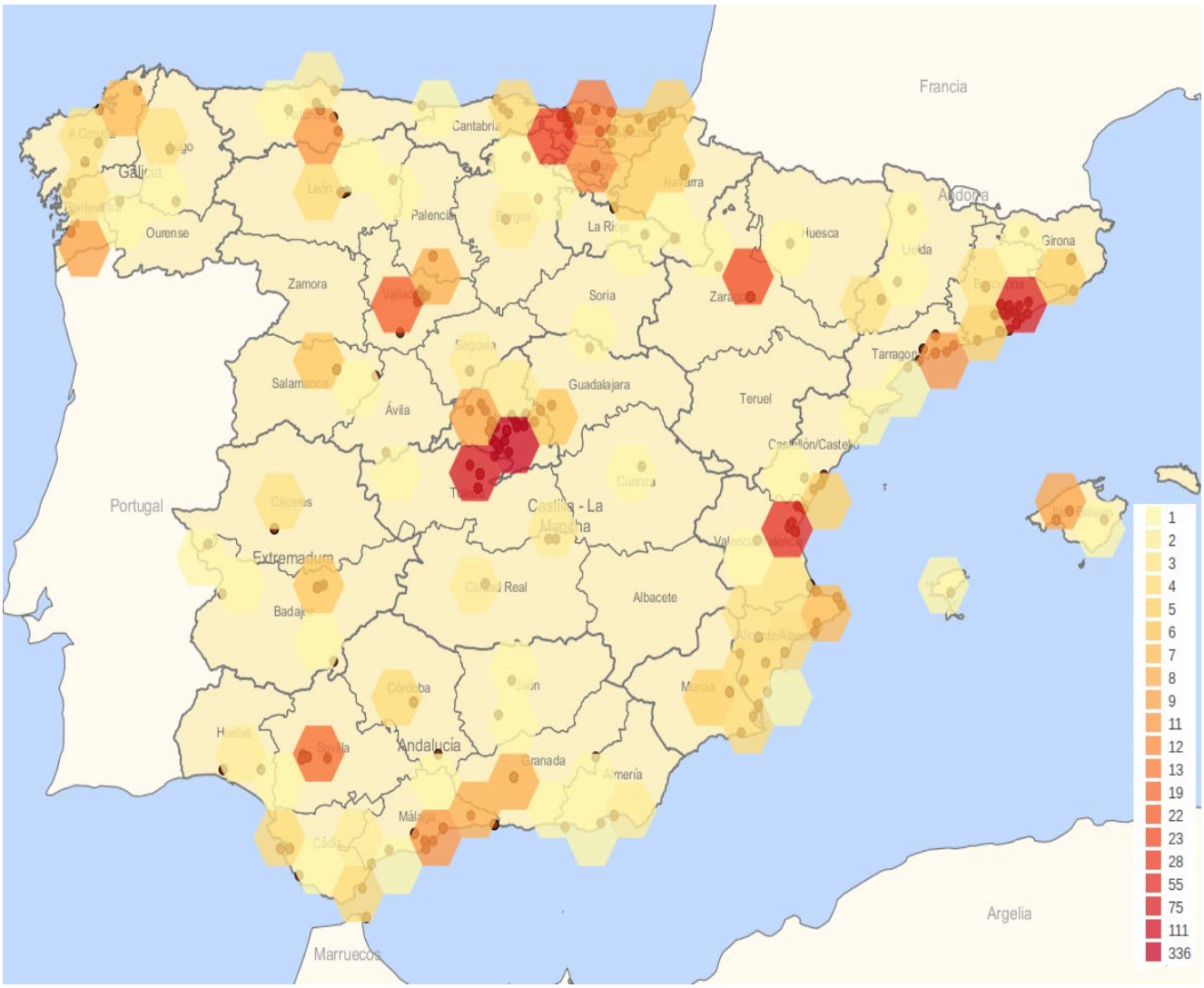
... es el sector relacionado con la Administración Pública el que presenta más elementos susceptibles de ataque desde Internet, seguido de la industria química y el sector energético.

Los sectores que menos debilidades presentan, al menos en función de los datos de entrada asociados a clasificación por sector estratégico, son el financiero y tributario, el espacial y el nuclear; en ninguno de ellos se han encontrado elementos considerados inseguros por este equipo, al menos con los datos anteriormente referenciados. Confiamos y deseamos que si cruzamos datos de sistemas de control con sectores estratégicos –trabajo casi por completo manual y que de momento no está previsto abordar– estos números se mantengan, ya que nos ha sorprendido gratamente la seguridad que a priori presentan estos tres sectores.

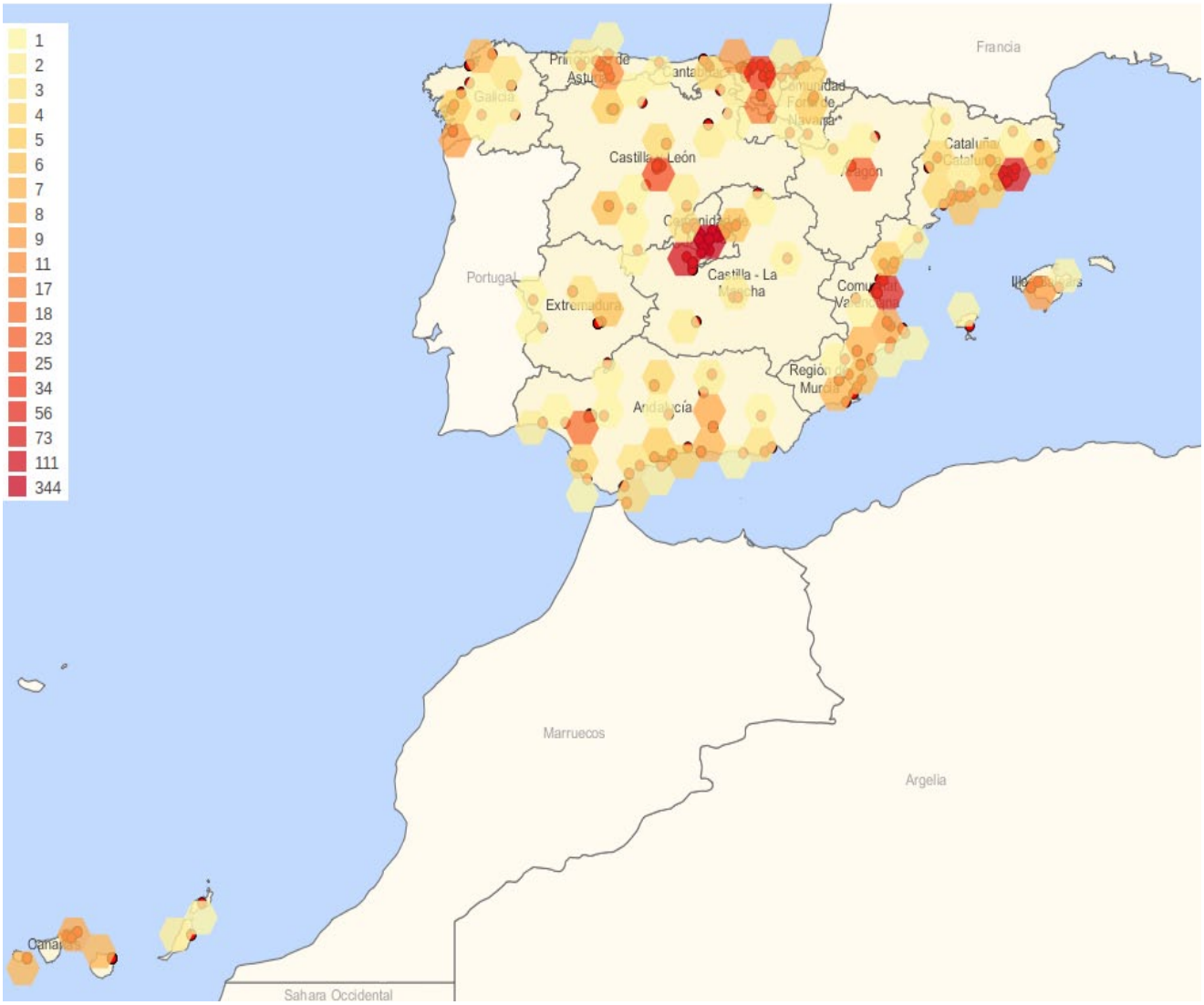
El hecho de que no existan entradas asociadas al sector TIC puede dar una falsa sensación de seguridad. Simplemente, tal y como se ha indicado con anterioridad, no están reflejadas en el análisis porque es muy difícil determinar de forma automática y con una baja probabilidad de error qué elementos de una tecnológica están asociados a infraestructuras críticas y qué elementos no lo están. De hecho, este equipo considera, a la vista de los datos adquiridos durante el estudio, que el tecnológico es uno de los sectores estratégicos que más graves deficiencias de seguridad presenta, tanto en sus propias infraestructuras como en las que prestan servicio a operadores críticos; un hecho muy significativo es el elevado número de elementos de comunicaciones operados por grandes tecnológicas que prestan servicio esencial en sectores estratégicos y que presentan debilidades muy significativas para nosotros, como el uso de protocolos en texto claro o simplemente la posibilidad acceso al mismo desde cualquier punto de Internet.

5.3 Mapas de densidad

A partir de las coordenadas GPS (cuya estimación también proporciona SHODAN) de los resultados aún en activo, se ha confeccionado un mapa de densidad mediante la herramienta de cartografía QGIS. El mapa indica la concentración de resultados por zona, siendo las zonas rojas las que más concentración poseen. Como es lógico, coinciden con las principales capitales y zonas más industrializadas del país: Madrid, Barcelona, Valencia y Bilbao y, en menor medida, Zaragoza y Sevilla.



Se muestra a continuación un detalle de la península y las Islas Canarias:



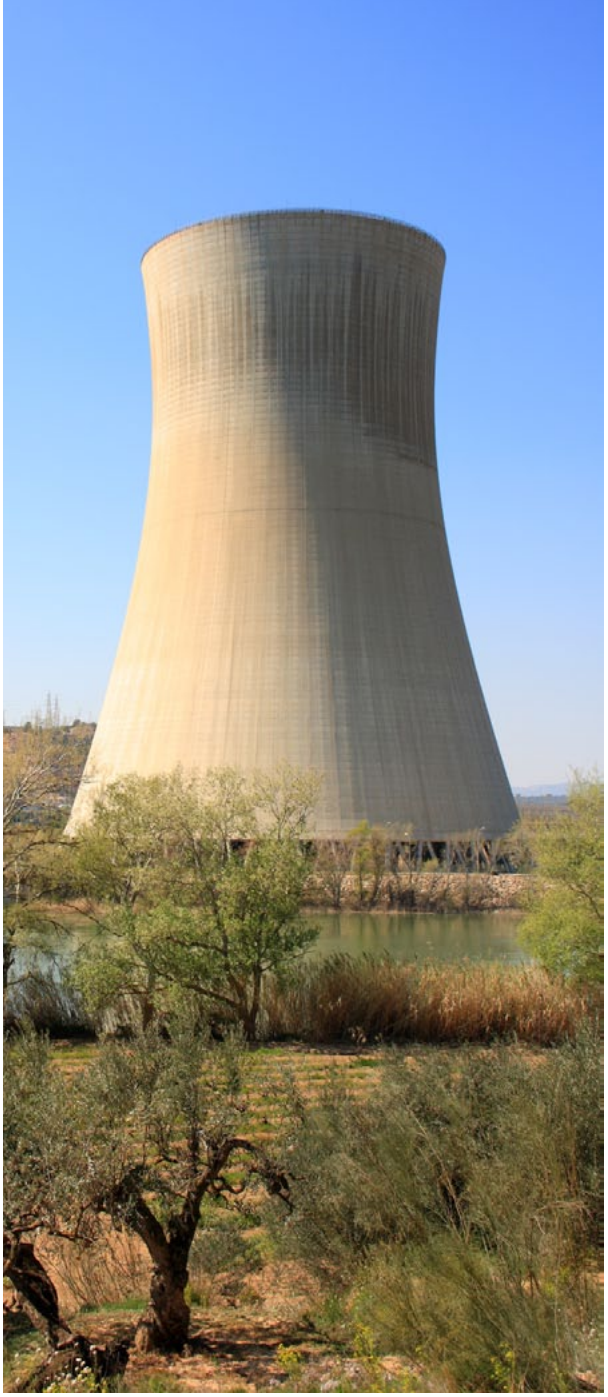
6. Conclusiones

6.1 Resumen

Una de las conclusiones de nuestro anterior informe sobre Protección de Infraestructuras Críticas en España era la necesidad de mejorar la seguridad lógica de las infraestructuras críticas, haciendo especial hincapié en la protección adecuada de los sistemas de control. Nos reafirmamos en esta conclusión, ya que el número de elementos tecnológicos asociados a infraestructuras críticas en España que han sido detectados mediante nuestro análisis es, a todas luces, demasiado elevado.

Pensemos que estamos hablando de más de 1.000 elementos que introducen , según nuestro criterio, debilidades en la seguridad lógica de infraestructuras críticas, en especial en lo que respecta a sistemas de control de uno u otro tipo. Alguien puede plantearse que si no hay vulnerabilidades en los sistemas de las infraestructuras críticas y presentan modelos de autenticación y cifrado aceptables, no deberían considerarse debilidades, pero seguimos opinando que simplemente tener la posibilidad de acceso a estos entornos desde Internet es en la mayor parte de casos algo no justificado y representa un potencial problema de seguridad a considerar.

Queremos hacer hincapié en que estos resultados son los obtenidos a partir de un análisis generalista –no se ha buscado en ningún momento un objetivo de evaluación concreto, un operador o infraestructura particular– basado en un conjunto de firmas y en unas técnicas de adquisición de datos al alcance de cualquiera, obviamente sin ejecutar pruebas hostiles y con un fin puramente muestral. No obstante, no se buscaba mediante este informe obtener una estadística matemáticamente perfecta, sino hacernos una ligera idea de lo que tenemos en materia de seguridad lógica en las infraestructuras críticas de nuestro país.



Por supuesto, el no profundizar en ninguno de los análisis puede inferir errores ya que, ¿quién nos dice que ese sistema SCADA aparentemente en una subestación de distribución eléctrica no era un simple *honeypot* o un entorno de pruebas aislado del de producción? Sin embargo, dudamos que este margen de error sea elevado; nuestra percepción sigue siendo que existe una debilidad lógica generalizada en algunas infraestructuras críticas, en muchos casos pequeñas –aunque también hemos tenido hallazgos de elementos asociados a grandes infraestructuras- pero en las que un ataque real y organizado puede causar un impacto elevado.

¿A qué puede ser debida esta situación, en la que un estudio generalista es capaz de "tocar" más de 1.000 elementos a priori sensibles, en mayor o menor medida, para la seguridad de infraestructuras críticas españolas?

¿A qué puede ser debida esta situación, en la que un estudio generalista es capaz de "tocar" más de 1.000 elementos a priori sensibles, en mayor o menor medida, para la seguridad de infraestructuras críticas españolas? Bajo nuestro punto de vista entran en juego tres factores fundamentales –luego hablaremos de un cuarto– que son el desconocimiento, la comodidad (ni siquiera queremos llamarle funcionalidad) y la inseguridad por defecto. Todos ellos se pueden resumir en uno único: la **falta de percepción del riesgo**.

Cuando hablamos de **desconocimiento**, nos referimos a que en muchas ocasiones los operadores de infraestructuras críticas no son conocedores de que una situación como las analizadas en este trabajo, con elementos relevantes para la seguridad expuestos en mayor o menor medida a Internet, pueda existir en sus infraestructuras y, si saben que puede existir, no son conscientes del riesgo que implica. Peor aún sería que fueran conscientes de este riesgo y lo asumieran, cosa que confiamos en que no suceda: queremos creer que si a una persona con responsabilidad en una infraestructura crítica se le explica que cualquiera, desde cualquier parte del mundo, puede probar contraseñas de acceso al router que gestione la conexión entre la infraestructura e Internet hasta que averigüe la correcta, o peor todavía puede directamente entrar a ese elemento o a un sistema SCADA y alterarlo a su antojo, se preocuparía (y mucho) y trataría de mitigar este riesgo.

El segundo gran factor al que hacíamos referencia es la **comodidad**; es más sencillo para el equipo que tiene que acceder a administrar los elementos tecnológicos poderlo hacer desde cualquier punto de Internet de forma directa, sin mecanismos previos de autenticación robusta o cifrado de datos, sin sistemas intermedios de salto y sin nada parecido que pueda complicar la operativa. Es más cómodo gestionar un SCADA desde un iPad, a través de la WiFi de un hotel y conectando a su interfaz gráfico que desplazarme físicamente a una sala de control, ubicada en la propia infraestructura crítica. Por supuesto, esto es así: es más cómoda una situación que la otra –aun tratándose de ejemplos extremos – pero creemos que degradar la seguridad en beneficio de la comodidad hasta este punto acabará siendo un problema.

Resulta necesario buscar soluciones intermedias que lleguen a un equilibrio entre la operación y la protección, soluciones que casi siempre existen. Pero si en algún caso no existen, consideramos que al menos en las infraestructuras críticas, debe primar siempre la seguridad.

Finalmente, tenemos la **inseguridad por defecto** de muchos sistemas. Estamos en un mundo en el que, cada vez más, conectamos todo a Internet: nos da igual un elemento troncal de comunicaciones, un sistema SCADA o el acuario o la nevera de nuestro domicilio. Si ese sistema de control o esa pecera son inseguros por defecto muy probablemente se mantendrán inseguros en su entorno operativo: despliego el sistema y directamente funciona, con lo que para qué preo-

cuparse de nada más; tenemos nuestra nueva impresora a la que se van a lanzar trabajos clasificados, la desembalamos, la enchufamos y la conectamos a la red. A través de DHCP se le asigna una dirección IP y mágicamente todo funciona, por lo que seguimos con nuestro trabajo y no nos damos cuenta de que esa impresora permite accesos de administración a través de TELNET o HTTP sin ninguna autenticación, con lo que cualquiera puede copiar nuestros trabajos, enviarlos por correo a cualquier cuenta o sencillamente apagarle. Veremos luego que el ejemplo de la impresora no es una elección al azar.

Evidentemente, los fabricantes de sistemas en general, pero sobre todo los que van a ser usados en infraestructuras críticas –por ejemplo, SCADA– deben reforzar la seguridad por defecto del despliegue de sus productos, pero también quienes los instalan o gestionan deben preocuparse de que, con independencia de lo que ha hecho o dicho el fabricante, estos sistemas se implanten y se operen de forma segura; no es de recibo que en pleno siglo XXI tantos y tantos elementos tengan entornos de administración a través de HTTP (y no de HTTPS), que presenten contraseñas por defecto o que siga existiendo tráfico TELNET.

...en algunas organizaciones que disponen de grandes rangos de red (como una clase B) encontramos dispositivos con direccionamiento público para los que no existe explicación –o no la hemos encontrado- que justifique ese direccionamiento

Para acabar, nos ha llamado la atención la presencia de algunos elementos para los que no se encuentra ninguna justificación al menos por nuestra parte, no ya para ser accesibles o no desde Internet, sino directamente para disponer de direccionamiento público. En algunas organizaciones que disponen de grandes rangos de red (como una clase B) encontramos dispositivos con direccionamiento público para los que no existe explicación alguna –o no la hemos encontrado– que justifique ese direccionamiento. Si a eso añadimos que algunas de estas organizaciones no disponen de elementos básicos de seguridad perimetral nos encontramos situaciones tan absurdas como una impresora –aparentemente departamental y que dudamos que se use desde otro sitio, y menos desde fuera de la red corporativa– que es completamente accesible desde Internet en sus puertos de administración y que para empeorar las cosas, no dispone de autenticación. Un atacante, desde cualquier lugar del mundo, puede directamente copiarse los trabajos impresos a través de un sencillo interfaz web.

6.2 Un problema de base

Aparte de los tres factores mencionados (desconocimiento, comodidad e inseguridad por defecto), consideramos que existe un factor de base adicional, no tan cercano al ámbito TIC pero con buena parte de culpa en la inseguridad de las infraestructuras críticas nacionales. Este es justamente la forma en que se ejecutan gran parte de las obras públicas en España (muchas de las cuales serán, probablemente, infraestructuras críticas): se trata del proceso de construcción en tres fases, proyecto, obra y explotación.

En demasiadas ocasiones estas fases constituyen compartimentos estancos con escaso flujo de información. Durante la construcción intervienen la consultora de ingeniería redactora del proyecto, la empresa contratista y sus subcontratas y proveedores, la Administración adjudicataria a través de sus directores de contrato y obra y sus asistencias técnicas. En la gran mayoría de los casos los máximos responsables de las obras son personas con gran formación y experiencia en el ámbito de la obra civil, pero con muy poca en cuestiones industriales y de sistemas de control. Por tanto, las empresas subcontratistas y proveedores poseen en este ámbito una autonomía mucho mayor de la que sería deseable y es posible que acciones como la arquitectura de los sistemas, conexión a Internet de un sistema de control, contraseñas, configuración de perfiles, etc. se tomen por personas que ni tienen la visión global necesaria ni la conciencia de la importancia de las mismas (hemos visto como se utiliza la posibilidad de conexión a Internet de un sistema de control, totalmente innecesaria por otra parte, como argumento de venta).

Todavía peor, las personas que intervienen en la construcción pierden el contacto con la obra tan pronto ésta termina, siendo sustituidas por otras que se dedicarán a gestionar la explotación y que normalmente se enfrentan a su trabajo con un conocimiento

limitado de las decisiones que se tomaron durante la construcción y la realidad de las instalaciones ejecutadas. Dicho de otra forma, el sistema conectado a Internet que hemos mencionado quedará así, configurado por defecto y sin conocimiento de los responsables, durante mucho tiempo.

Por último, no hay que perder de vista, además, que cada participante posee sus propios intereses (la empresa explotadora se centrará en aquellas tareas que tengan repercusión inmediata en la determinación de su remuneración, por ejemplo) razón por la cual decisiones erróneas en fases previas a la explotación quedan 'fosilizadas', ya que no es evidente la relación entre el esfuerzo dedicado a labores como éstas y la remuneración percibida (el coste de la no seguridad). Por tanto en ésta, como en otras cosas, la solución debe partir de la propia Administración adjudicataria, que debe fijar unos criterios claros y dar relevancia a esta cuestión a través de los Pliegos y de la concienciación de los agentes en todas las fases del proceso proyecto – construcción – explotación.

... es un problema especialmente grave en las obras promovidas por el sector público, donde incluso se da el caso de obras adjudicadas por una Administración que posteriormente son cedidas para su explotación y conservación a otra entidad pública diferente.

Éste es un problema especialmente grave en las obras promovidas por el sector público, donde incluso se da el caso de obras adjudicadas por una Administración que posteriormente son cedidas para su explotación y conservación a otra entidad pública diferente. Sin embargo, la participación privada no mejora las cosas *per se*. Es cierto que en las obras promovidas por compañías de este sector la integración a lo largo del proceso es mucho mayor, como es el caso, por ejemplo, de la construcción de centrales de generación promovidas por compañías eléctricas en las cuales hay participación directa en labores de coordinación y supervisión por parte de la propiedad, que en última instancia acabará explotando la obra. Pero en otras ocasiones, la empresa privada a cargo de la explotación antepone sus necesidades (que no tienen por qué ser ilegítimas) a las del titular de la infraestructura, momento en el que surgen situaciones de riesgo. Por ejemplo, los esfuerzos por acotar perfectamente el perímetro lógico de un sistema de control pueden entrar en conflicto con la necesidad de mantenimiento del mismo, lo que da lugar a la aparición de conexiones a Internet no controladas (como módem 3G, etc.). Conocemos casos de servidores de sistemas de control infectados, a sabiendas del explotador, por virus imposibles de eliminar al no existir la posibilidad de mantener las bases de datos de los antivirus actualizadas ya que dichos servidores no están conectados a Internet.

6.3 Líneas futuras de trabajo

Las líneas de trabajo que este equipo considera prioritarias son justamente las dedicadas a mitigar los factores descritos con anterioridad; como objetivo general, las personas y equipos involucrados en la protección de infraestructuras críticas deben ser plenamente conscientes de los riesgos derivados del ámbito tecnológico, al igual que confiamos en que lo sean de los riesgos derivados de cualquier otro ámbito de la seguridad. Si no asumimos y comprendemos que a través de canales lógicos un atacante puede causar el mismo o más impacto que a través de otros canales, y que por tanto debemos hablar de una protección global y proporcional en todos sus ámbitos para las infraestructuras críticas, creemos que poco más podemos hacer. No es permisible el desconocimiento y este es un trabajo de **formación** y **concienciación** en seguridad dirigido a todos los actores con el que deberíamos ser capaces de mitigar los problemas asociados al desconocimiento de los que antes hacíamos referencia.

Los aspectos derivados de la comodidad no deben anteponerse jamás a los aspectos relativos a la seguridad en infraestructuras críticas; por supuesto, no se trata de perjudicar porque sí a los equipos de trabajo que necesitan acceder de forma remota a sistemas de control o a cualquier otro elemento tecnológico de la infraestructura, ni de obstaculizar el desarrollo de sus funciones. Se trata, como siempre se suele decir, de que el equilibrio entre seguridad y comodidad –no le llamamos funcionalidad– sea correcto y en caso de duda, se prime a la seguridad siempre estableciendo **canales de acceso seguro** a los elementos tecnológicos de las infraestructuras críticas.

Hace ya años que existen diferentes mecanismos que permiten este acceso remoto seguro a cualquier elemento –o casi–, incluso a través de redes de propósito general, por lo que consideramos incorrecto acceder a través de Internet directamente a interfaces de administración –a través del protocolo que sea– de elementos tecnológicos, de control industrial o de propósito general, asociados a infraestructuras críticas (aunque como hemos dicho podríamos extrapolar esta afirmación a cualquier otra infraestructura). Sencillamente, una simple VPN que controle y refuerce el acceso externo a las plataformas supondría un salto cualitativo muy importante para la seguridad lógica de las infraestructuras críticas.

Debemos exigir a los fabricantes, proveedores, operadores, instaladores o cualesquiera actores involucrados en esta inseguridad por defecto un cambio sustancial que evite situaciones como las vistas en este informe técnico

En relación a la inseguridad por defecto de tantos y tantos elementos, consideramos, como hemos dicho antes, que en pleno siglo XXI directamente no deben aceptarse en una infraestructura tecnológica (considerada crítica o no) elementos sensibles –o potencialmente sensibles– que presenten protocolos de acceso para gestión de los elementos en texto claro, sin autenticación o incluso con contraseñas por defecto. A partir de este punto, podemos seguir hablando de seguridad, pero consideramos que estos serían los requisitos mínimos exigibles en todo caso. Debemos exigir a los fabricantes, proveedores, operadores, instaladores o cualesquiera actores involucrados en esta inseguridad por defecto un cambio sustancial que evite situaciones como las vistas en este informe técnico.

Finalmente, los problemas asociados al proceso de construcción deben abordarse mejorando el flujo de información y la coordinación a lo largo de todo el proceso de diseño, construcción y explotación de las infraestructuras críticas, estableciendo criterios y una **supervisión y coordinación** claras por parte del titular desde la misma concepción de la instalación.

Como tantas otras veces, si cada uno de los actores involucrados se limita a su ámbito estricto, sin una responsabilidad claramente definida por encima de él, difícilmente podremos hablar de seguridad global en el proceso, con lo que seguiremos arrastrando problemas de raíz que la tecnología podrá corregir en algunos casos, pero no en otros.

El objetivo final que creemos que mucha gente persigue –perseguimos– desde el punto de vista técnico es, simplificando mucho, que una captura de pantalla como la siguiente (se han eliminado datos de modelo, fabricante, etc.) sea difícil o imposible de realizar a través de Internet:

Variable 1

OID: .1.3.6.1.4.1.4576.4.6.1.1.1.0
Tipo: GAUGE
Descripción: Tension fotovoltaica
Actualizar Borrar

Variable 2

OID: .1.3.6.1.4.1.4576.4.6.1.1.3.0
Tipo: GAUGE
Descripción: Corriente de entrada
Actualizar Borrar

Variable 3

OID: .1.3.6.1.4.1.4576.4.6.1.1.24.0
Tipo: GAUGE
Descripción: Potencia activa
Actualizar Borrar

Variable 4

OID: .1.3.6.1.4.1.4576.4.6.1.1.37.0
Tipo: GAUGE
Descripción: Temperatura ambiente
Actualizar Borrar

Variable 5

OID: .1.3.6.1.4.1.4576.4.6.1.1.6.0
Tipo: GAUGE
Descripción: Tension de red Fase R
Actualizar Borrar

Variable 6

OID: .1.3.6.1.4.1.4576.4.6.1.1.7.0
Tipo: GAUGE
Descripción: Tension de red Fase S
Actualizar Borrar

Variable 7

OID: .1.3.6.1.4.1.4576.4.6.1.1.8.0
Tipo: GAUGE
Descripción: Tension de red Fase T
Actualizar Borrar

El anterior es un ejemplo de entorno de control accesible vía HTTP, desde cualquier punto de Internet y sin ningún tipo de autenticación; no sabemos qué implicaría modificar o borrar alguno de los parámetros anteriores ni cómo afectaría esto –u otras alteraciones posibles– al comportamiento del sistema de control. Es más, ni siquiera podemos asegurar a ciencia cierta que este SCADA esté realmente en una infraestructura crítica… pero mucha gente con malas intenciones lo puede estar comprobando en este mismo momento.

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] Informe Protección de Infraestructuras Críticas 2011. S2 Grupo. Diciembre de 2011.

Contacto
Antonio Villalón Huerta
Director de Seguridad
S2 Grupo

avillalon@s2grupo.es
www.s2grupo.es