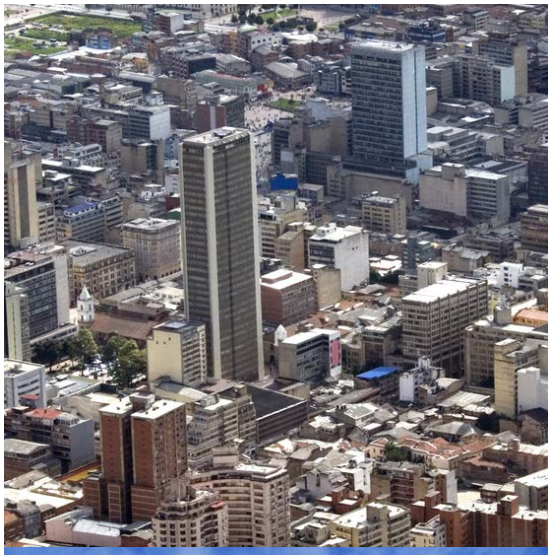
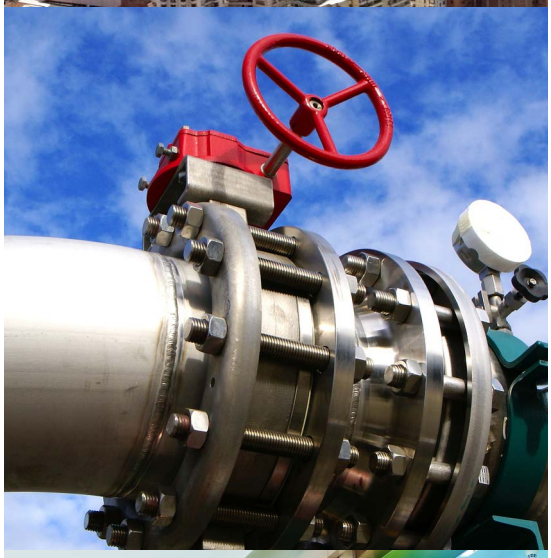
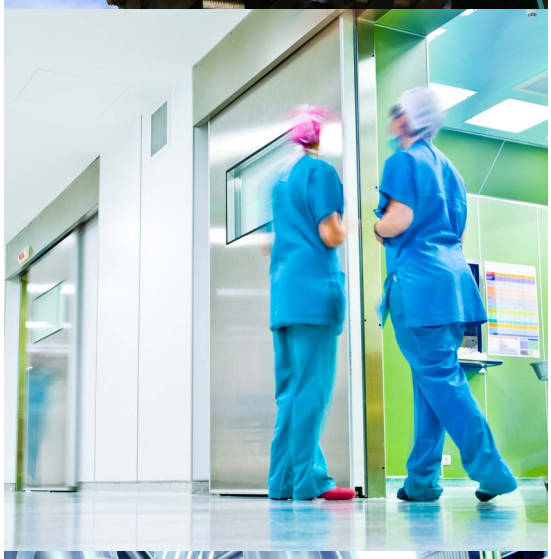






Protección de Infraestructuras Críticas en Colombia

Informe Técnico - Febrero 2013

GRUPO

Sobre S2 Grupo

S2 Grupo es una empresa especializada en ciberseguridad, considerada como un medio para la protección de los activos de información de sus clientes y de sus procesos de negocio. Tiene una amplia experiencia en el desarrollo de productos y la prestación de servicios de ciberseguridad a empresas de tamaño medio o grande, corporaciones y administraciones públicas.

S2 Grupo ha obtenido la certificación en los referenciales más importantes: ISO 9001 (Sistema de Gestión de Calidad), ISO 27001 (Sistema de Gestión de Seguridad de la Información) e ISO 20000 (Gestión de Servicios TIC).

S2 Grupo dispone de oficinas en Madrid, Valencia, Bogotá y Bucarest. En Valencia se encuentra su Centro de Operaciones de Seguridad (SOC) y sus instalaciones de proceso de datos.

Autores
Antonio Villalón
Pablo Marín

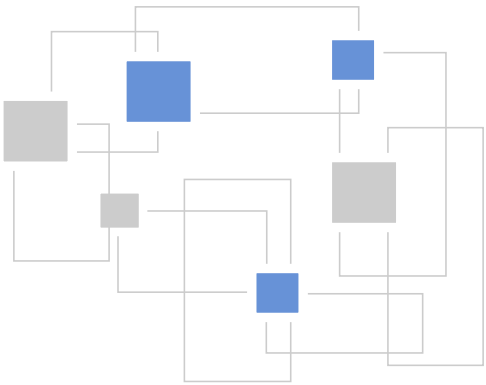
Diseño y maquetación
Karina Coste

Fecha de publicación
Febrero 2013

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

Contenido

1. Introducción



En diciembre de 2011, S2 Grupo publicaba su primer informe sobre Protección de Infraestructuras Críticas, en el que se analizaba la situación internacional –con especial hincapié en la española– en la materia, principalmente normativa, y se planteaban líneas de trabajo a desarrollar para seguir lo que estimamos es la dirección correcta en el ámbito de la PIC.

Este trabajo se complementaba en noviembre de 2012 con un informe técnico sobre la protección de infraestructuras críticas en España, con un enfoque 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 la realización de este informe considerábamos inseguro cualquier elemento accesible desde Internet –independientemente de su esquema de autenticación, si lo tiene– y que a priori, bajo nuestro criterio particular no debía estarlo. En otras palabras: por razones obvias el servidor de correo de una organización debe estar disponible desde cualquier punto de Internet, pero no deben estarlo sus sistemas SCADA o los dispositivos de comunicaciones troncales.

De esta forma, en el informe técnico realizábamos un análisis exclusivamente técnico de la información públicamente disponible en Internet, mediante la revisión práctica de aquellos elementos a priori sensibles que pudieran introducir riesgos en las infraestructuras críticas españolas. En ningún caso se realizaron pruebas que podrían considerarse hostiles (análisis de visibilidad, prueba de contraseñas por defecto…) contra esas mismas infraestructuras.

El objetivo del informe no era otro que tener una estimación aproximada de hasta qué punto, sin ejecutar pruebas hostiles ni lanzar ataques complejos contra nadie, los elementos que formaban parte de las infraestructuras críticas estaban expuestos a agentes externos a su gestión.

Los resultados del informe técnico de S2 Grupo fueron muy claros: es preocupante, y mucho, la seguridad lógica de las infraestructuras críticas españolas; existen situaciones de riesgo, siempre bajo nuestro punto de vista, que son únicamente achacables a una falta de percepción del riesgo real y no a lo que podríamos considerar limitaciones de carácter técnico o de otra índole.

“En febrero de 2013, hemos trabajado en un análisis equivalente al descrito, pero focalizado en esas mismas infraestructuras en Colombia. En este sentido, el presente informe debe considerarse como un estudio particularizado para el caso colombiano, pero manteniendo la metodología utilizada y descrita en el informe técnico mencionado. Aunque en el presente documento se indican de manera resumida los principales aspectos, se remite al lector interesado en un mayor nivel de detalle a dicho documento.

En relación con los resultados obtenidos, como se verá durante el desarrollo de este informe estos han sido, desafortunadamente, muy similares: en Colombia, al igual que en España, queda mucho trabajo por desarrollar en el ámbito de la protección de infraestructuras críticas.”

2. Planificación y metodología

Para la ejecución de nuestro estudio hemos tratado de identificar elementos significativos asociados a infraestructuras críticas en Colombia que puedan ser accesibles de una u otra forma desde Internet, y por tanto atacados.

Como elemento de guía en lo referente a los sectores, se ha tomado como base la Ley 8/2011 española, transposición de la Directiva Europea 2008/114/CE, en particular en aquellos aspectos relacionados con la identificación y clasificación de las infraestructuras críticas. Entendemos que con independencia de la situación particular y organización política de cada estado, como puede ser Colombia en este caso, los sectores estratégicos relacionados con las infraestructuras críticas son en esencia los mismos.

Desde este punto de vista, estos son los sectores estratégicos identificados:

- Administración pública
- Espacio
- Industria Nuclear
- Industria Química
- Instalaciones de Investigación
- Agua
- Energía
- Salud
- Tecnologías de la Información y las Comunicaciones (TIC)
- Transporte
- Alimentación
- Sistema Financiero y Tributario

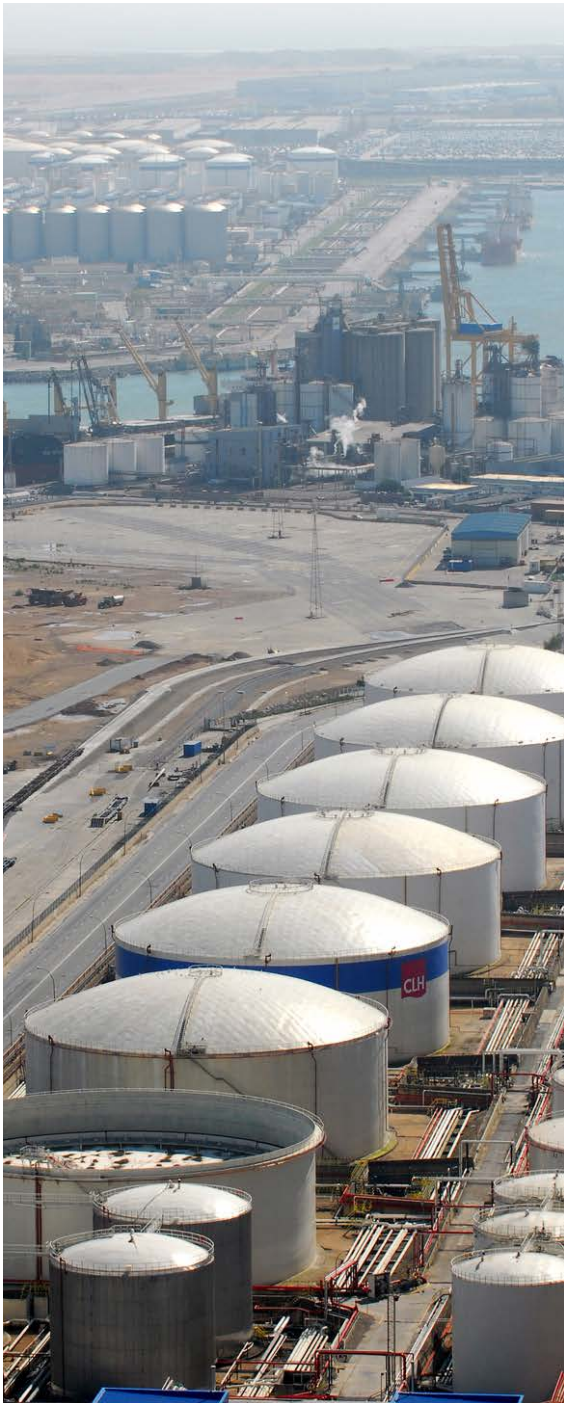
Siguiendo la metodología del informe PIC 2012, de cada uno de estos sectores estratégicos queremos identificar aquellos elementos tecnológicos públicamente disponibles en Colombia. Aunque la metodología es básicamente la misma utilizada en el informe PIC 2012 con ligeras modificaciones, que no creemos útil repetir en este informe, vamos a dar algunas pinceladas sobre ella, remitiendo al lector interesado en un mayor nivel de desarrollo al informe citado, descargable desde la página web de S2 Grupo.

El proceso de identificación comienza mediante la elaboración de patrones o firmas de dispositivos utilizados habitualmente en infraestructuras críticas o sectores estratégicos, para lo cual se han utilizado dos fuentes de información. Por un lado, se han analizado entre otros los principales fabricantes, sistemas PLC, terminales táctiles y software de control utilizados en los sistemas SCADA. Por otro, se ha utilizado la recopilación de productos y firmas realizada por el ICS-CERT (*Industrial Control Systems Cyber Emergency Response Team*) estadounidense, que se ha complementado con datos provenientes de fuentes propias.

El siguiente paso es la utilización de las firmas o patrones en el buscador SHODAN, limitando el alcance al ámbito de Colombia. Esto nos dará como resultado los datos de aquellos elementos asociados a infraestructuras críticas en Colombia, que es la entrada a un análisis posterior y permite tener una idea aproximada del volumen de información que podría llegar a conseguir un atacante sin ninguna infraestructura específica. Evidentemente, este no puede considerarse un medio totalmente fiable para determinar que un sistema de control está desplegado en una infraestructura crítica, pero tras una fase de eliminación de falsos positivos, es factible asumir que los resultados obtenidos pueden asociarse a este tipo de infraestructuras con una probabilidad alta.

La fase final consiste en el procesamiento de la información obtenida, con objeto de realizar un análisis de mayor altura y extraer conclusiones. Cabe destacar que el análisis de parte de los datos recabados sigue en proceso y no será publicado en abierto.

Como se ha indicado, aquellas personas interesadas en el detalle del proceso completo, consistente en la elaboración de firmas, adquisición de datos y procesamiento posterior, incluyendo la identificación de falsos positivos, pueden consultar el informe PIC 2012.



3. Resultado y análisis

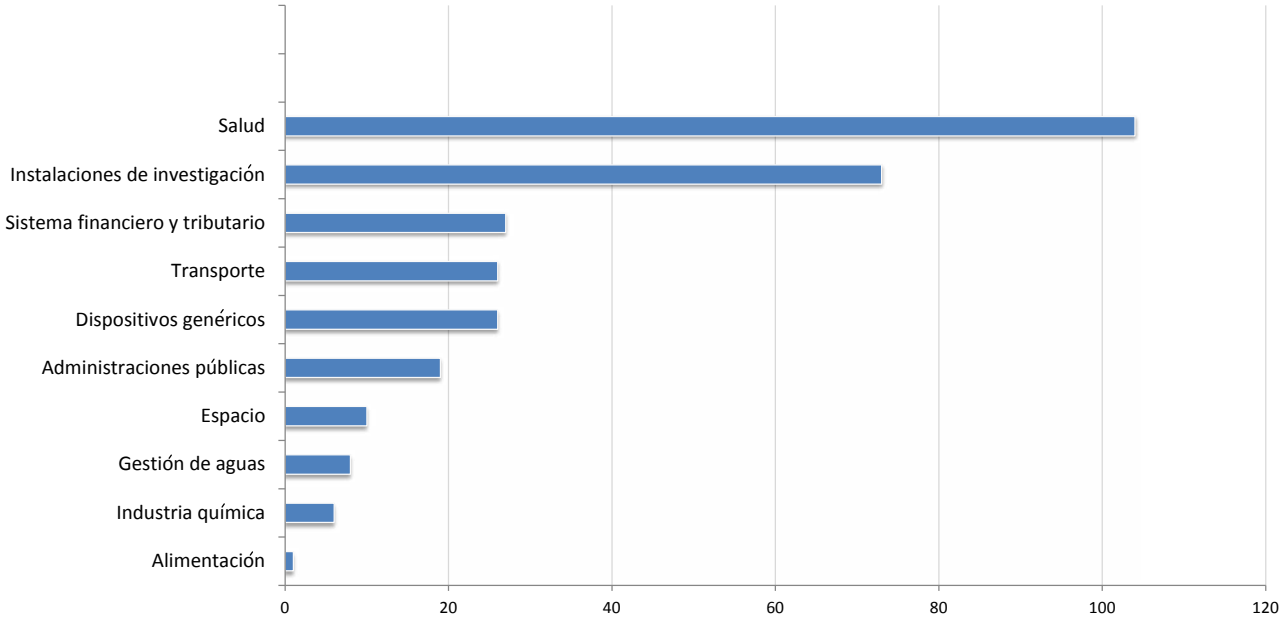
3.1 Resultados

Volvamos a la pregunta a la que este informe trata de dar respuesta:

¿Cuántas –potenciales– infraestructuras críticas colombianas presentan algún modelo de acceso remoto no adecuado para su seguridad y por tanto son susceptibles de ser atacadas directamente desde Internet?

Teniendo en cuenta que se ha invertido un esfuerzo considerable en la eliminación de ruido y falsos positivos en las fases previas, nos hemos encontrado **759 elementos** que de de algún modo se encuentran asociados a infraestructuras críticas y cuya visibilidad introduce, siempre bajo nuestro criterio, debilidades o directamente vulnerabilidades relevantes en la infraestructura afectada.

Se incluyen a continuación los resultados obtenidos para cada una de las firmas una vez se han eliminado falsos positivos, constituyendo un total de 759 resultados a fecha de redacción del presente informe. De este volumen, 370 entornos están asociados a sistemas de control (26 de ellos genéricos y 344 identificados por firmas de fabricantes) y los 389 entornos adicionales están asociados directamente a sectores estratégicos, según la siguiente distribución:

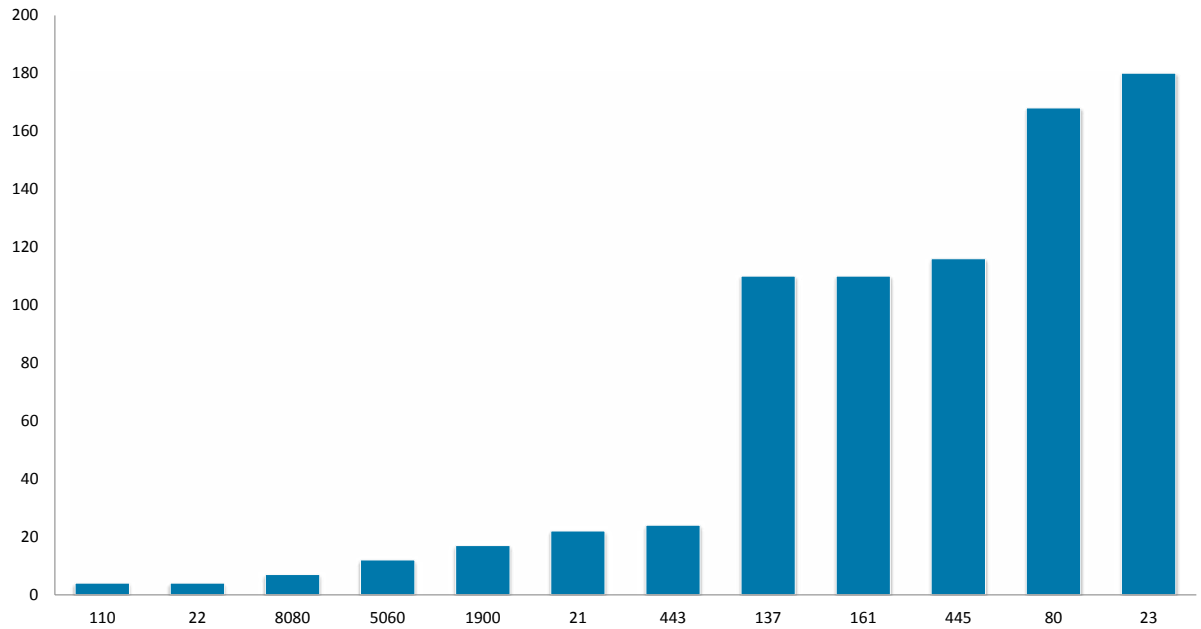


A partir de estos resultados, cabe realizar un análisis de los diferentes protocolos de acceso encontrados, sectores estratégicos identificados y mapas de densidad geográficos, que nos permitan establecer “zonas calientes” en la distribución de infraestructuras críticas en Colombia.

Estos tres aspectos son desarrollados a continuación.

3.2 Protocolos de acceso

Tomando 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:

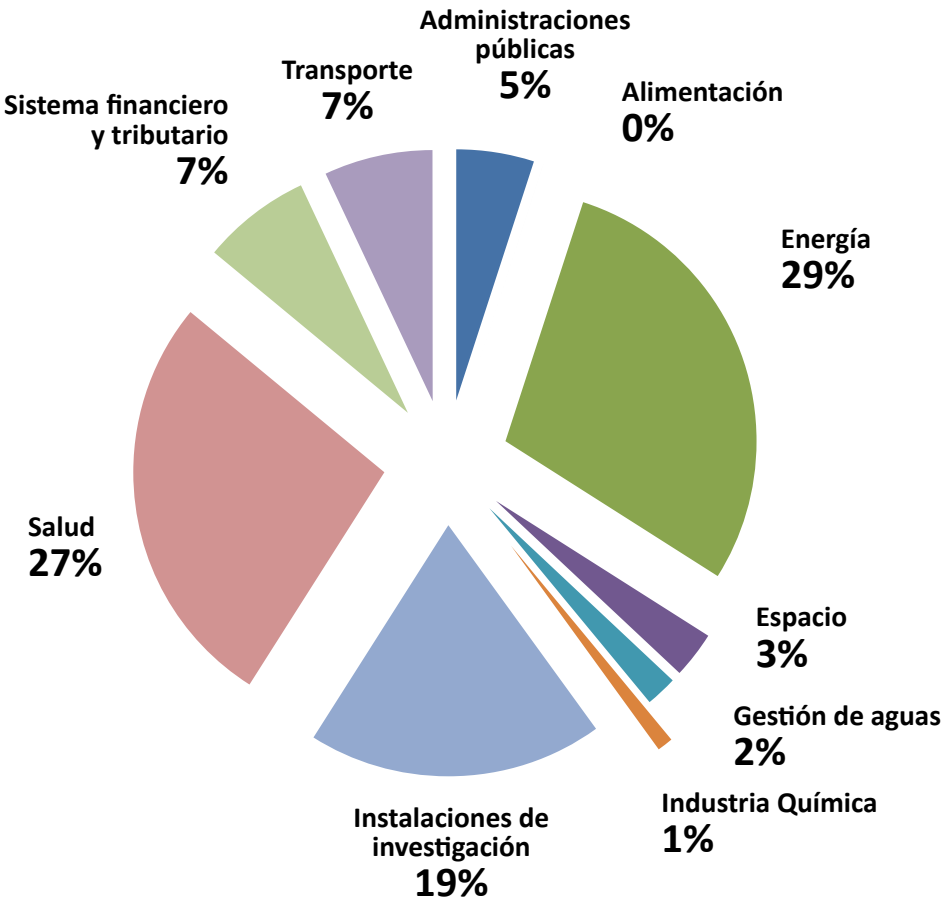


Como puede observarse, destaca enormemente el uso de protocolos en texto claro para acceder a entornos asociados a infraestructuras críticas; por ejemplo, el protocolo TELNET (puerto 23), utilizado habitualmente para acceso de terminal remota –privilegiado o no– o el protocolo HTTP (puerto 80) para acceso mediante un navegador web. Ninguno de estos protocolos incorpora cifrado de datos, así como tampoco lo hacen los protocolos SNMP (puerto 161) o FTP (puerto 21), por citar unos ejemplos. Desde el punto de vista del transporte cifrado de datos, sólo deberíamos considerar aceptable la disponibilidad de protocolos que cifren la información en tránsito y permitan autenticar los extremos, como es el caso de HTTPS (puerto 443). No obstante, acceder a un dispositivo de esta forma directamente desde Internet siempre introduce vulnerabilidades significativas y, tratándose de infraestructuras críticas, debería ser un modo de acceso prohibido por la política de seguridad corporativa.

Siguiendo con el protocolo TELNET, es también especialmente significativa la presencia de protocolos que permiten un alto grado de interacción –incluida la sesión remota– con los dispositivos; este es el caso de TELNET o SSH y, en menor medida, de los puertos asociados a NetBIOS (137 y 145). Ya sea de manera accidental o intencionada, exponer este tipo de protocolos a Internet introduce un nivel de riesgo difícilmente aceptable en el ámbito de las infraestructuras críticas.

3.3 Sectores estratégicos

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

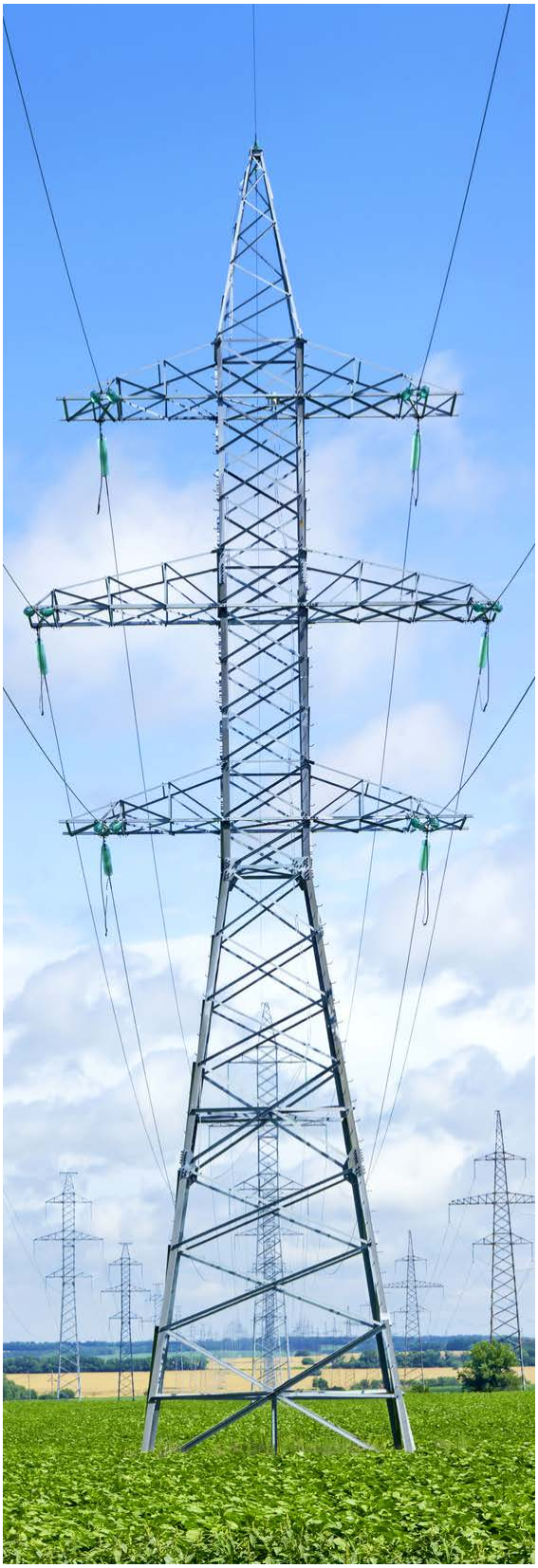


En este caso, debido a la imposibilidad de asociar de forma automatizada un elemento de control a un sector concreto, únicamente se han considerado como datos de entrada aquellos asociados a la clasificación de las firmas por sector estratégico, dejando fuera las correspondientes a elementos SCADA genéricos o de ciertos fabricantes.

Como podemos comprobar, los sectores de Salud y Energía son los más expuestos a Internet desde el ámbito de la ciberseguridad industrial, sumando entre ambos más de la mitad de los entornos encontrados durante este trabajo.

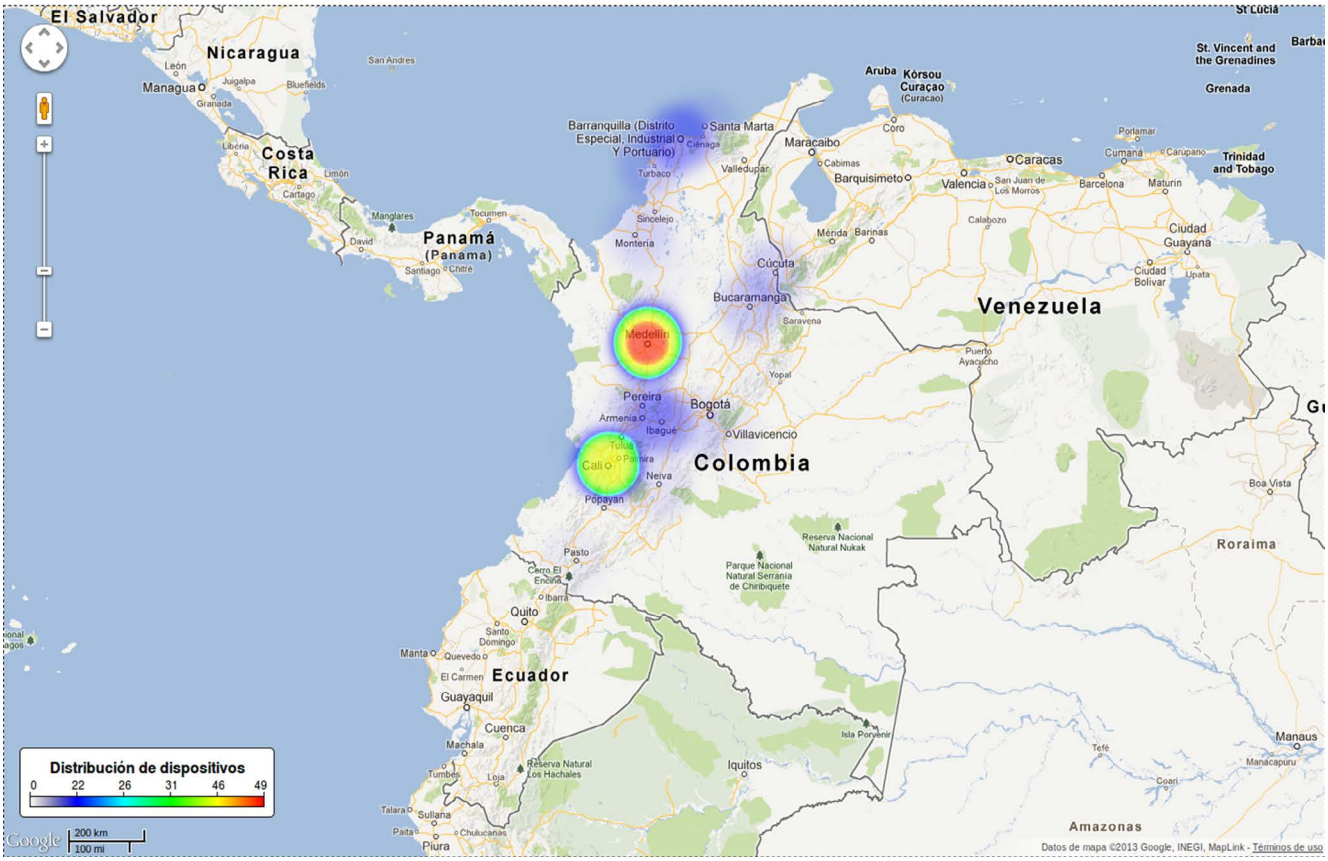
Adicionalmente, en los resultados cabe destacar dos ausencias significativas. Por un lado, la del sector TIC, lo que puede proporcionar una falsa sensación de seguridad. Sin embargo, lejos de la realidad, este hecho está asociado a la dificultad de determinar de forma automática y con una baja probabilidad de error, qué elementos de una tecnológica están asociados a infraestructuras críticas y qué elementos no lo están. De hecho, los datos obtenidos en ambos estudios (España y Colombia) muestran que la realidad es muy diferente, siendo el tecnológico uno de los sectores estratégicos con mayores deficiencias de seguridad presenta; se han detectado elementos de comunicaciones operados por grandes tecnológicas soportando servicios esenciales en sectores estratégicos que presentan debilidades muy significativas, como el uso de protocolos en texto claro o la posibilidad de acceso al mismo desde Internet.

En el extremo opuesto encontramos el sector Nuclear, también sin representación en la gráfica anterior pero en este caso por un motivo diferente: efectivamente, no hemos encontrado ningún sistema relevante que pudiéramos asociar a dicho sector de forma unívoca, por lo que debemos considerar, a priori, al sector nuclear como el más seguro de los analizados en Colombia.



3.4 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 calor mediante Google Maps; como es lógico, las tres zonas con mayor concentración de dispositivos conectados corresponden a la capital Bogotá, a Medellín y a Cali, que por supuesto son las tres mayores ciudades colombianas.



Como vemos, las mayores ciudades y zonas industriales del país tras las citadas previamente (esto es, Barranquilla, Cartagena, Cúcuta, Bucaramanga…) concentran, obviamente, la mayor población de elementos sensibles conectados a Internet.

4. Conclusiones

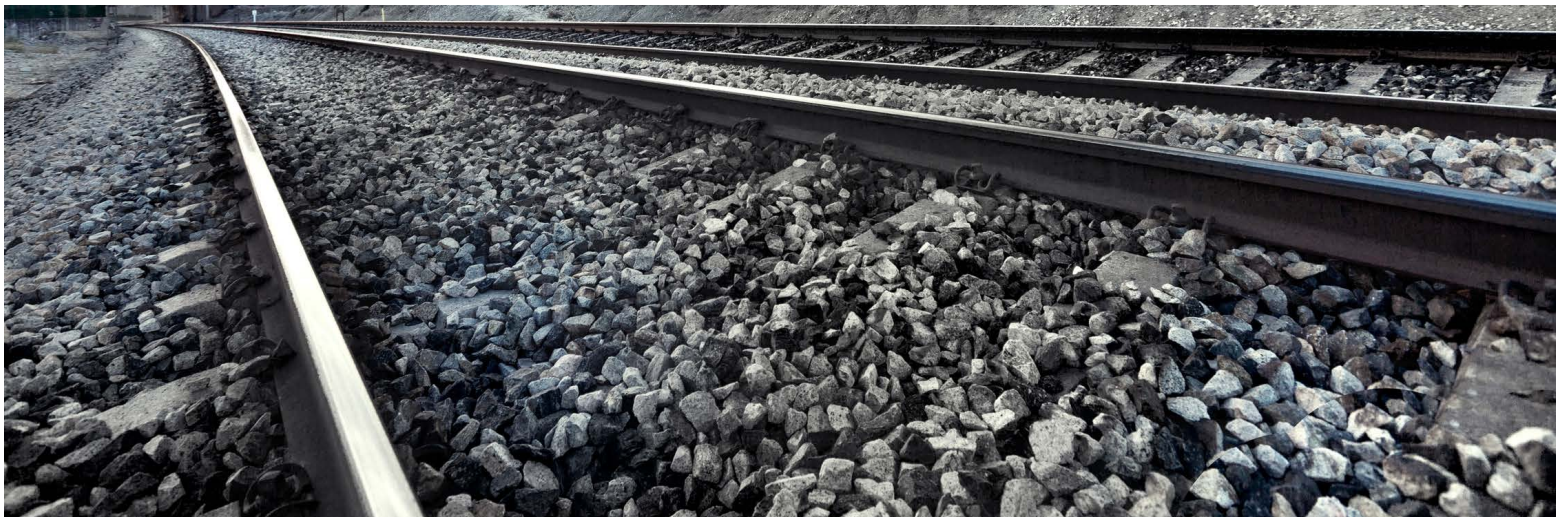
4.1 Resumen

Una de las conclusiones de nuestro anterior informe técnico PIC, equivalente al presente pero en el ámbito español, era la necesidad de mejorar la seguridad lógica de las infraestructuras críticas, haciendo especial hincapié en la protección adecuada de los sistemas de control.

Tras analizar la situación en Colombia, no hemos encontrado una situación mucho mejor, lo cual no es desgraciadamente ninguna sorpresa: los análisis de otras entidades en este ámbito no son muy optimistas con el estado de las IC en otros países, lo cual debería llevar a los Estados a actuar de manera decisiva sobre la seguridad de infraestructuras que son vitales para el bienestar de la ciudadanía y el funcionamiento del estado.

Es necesario destacar que los resultados han sido obtenidos a partir de un análisis generalista, sin centrarse en un objetivo de evaluación concreto y utilizando sistemas de adquisición de datos al alcance de cualquier usuario con acceso Internet. Si bien la falta de profundidad en el análisis (el sistema SCADA detectado en un centro de transformación eléctrica podía ser simplemente un entorno de pruebas) puede conducir a errores, pero dudamos que este margen de error sea significativo. Tanto nuestra percepción como la de otros especialistas en la materia es que la debilidad lógica de algunas infraestructuras críticas permitiría llevar a cabo un ataque real con un impacto elevado.

Para hablar de las causas de esta inseguridad, ya adelantamos en nuestro anterior informe que entran en juego tres factores fundamentales que se pueden resumir en uno único: la **falta de percepción del riesgo**; estos tres factores a los que hacemos referencia eran el **desconocimiento**, la **comodidad** (ni siquiera queremos llamarle funcionalidad)



y la **inseguridad por defecto**. Remitimos al lector a dicho informe para obtener los detalles de cada uno de éstos.

4.2 Líneas futuras de trabajo

Debido a que los resultados obtenidos están en la misma dirección de lo que se obtuvo en el anterior informe, las líneas a seguir no pueden, evidentemente, ser muy diferentes.

Todos los actores involucrados en la gestión de las infraestructuras críticas deben trabajar de manera conjunta para mitigar los factores identificados con anterioridad. En primer lugar, el personal involucrado en la protección de las IC debe conocer los problemas de seguridad que se derivan del ámbito tecnológico; el desconocimiento del riesgo que introduce un dispositivo conectado a Internet no es algo admisible si atendemos a las consecuencias. Este es sin duda un trabajo de **formación** y **concienciación** de largo alcance, en el que deben participar todos los actores relevantes en la gestión de las infraestructuras críticas.

En este sentido y desde el punto de vista del informe, la accesibilidad de dispositivos de IC desde Internet, debe alcanzarse un equilibrio entre seguridad y "comodidad" proporcional en todo caso a la importancia del elemento considerado. En el caso que nos ocupa, la seguridad debería siempre primar por encima de la "comodidad", y estableciendo siempre **canales de acceso remoto seguros** haciendo uso de mecanismos y protocolos disponibles desde hace años, como puede ser una simple VPN que controle y refuerce el acceso externo a las plataformas. Tan sólo con una medida así se mejoraría de manera muy significativa la seguridad lógica de cualquier infraestructura crítica.

Otro aspecto diferente es la inseguridad por defecto de muchos elementos utilizados en estas instalaciones, como puede ser el uso de protocolos de acceso para gestión de los elementos en texto claro, sin autenticación o incluso con contraseñas por defecto. Hablar de seguridad cuando estos aspectos no son todavía contemplados por los propios fabricantes impone muchas limitaciones a la seguridad de las IC y a las iniciativas que se desplieguen. Es imperativo que los agentes públicos y privados relevantes **exijan** a los fabricantes, proveedores, operadores, instaladores o cualesquiera actores responsables de esta inseguridad por defecto un cambio sustancial que evite situaciones como las vistas en este informe técnico.

Finalmente, no debemos olvidar los problemas derivados de la gestión del proceso de diseño y construcción de infraestructuras, generados por una ausencia de convergencia entre sectores y profesionales muy diferentes como son el industrial y el tecnológico –pero condenados a entenderse–, lo que conduce a la situación analizada en este informe. La solución, que requiere un cambio de filosofía en muchos casos, pasa ineludiblemente por mejorar 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. En el momento en el que cada actor involucrado se limita a su ámbito estricto, seguiremos arrastrando problemas difícilmente subsanables.

La ley 8/2011 española define el concepto de infraestructura crítica como aquella "*cuyo funcionamiento es indispensable […], por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales*" A su vez, define los servicios esenciales como aquellos servicios necesarios "*para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas*". Es evidente, por tanto, que las implicaciones de los resultados obtenidos en este informe, tanto en el caso español como en el colombiano, van mucho más allá del ámbito industrial o tecnológico, y limitarse a éstos sería un error con graves consecuencias para el conjunto de la sociedad.

Referencias

[1] Informe Técnico de Protección de Infraestructuras Críticas 2011. S2 Grupo. Diciembre de 2012.

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

Usted es libre de
Copiar, distribuir y comunicar públicamente la obra
Remezclar *— transformar la obra*
Hacer un uso comercial de esta obra

Bajo las condiciones siguientes:

Reconocimiento — *Debe reconocer los créditos de la obra de la manera especificada por el autor o el licenciador (pero no de una manera que sugiera que tiene su apoyo o apoyan el uso que hace de su obra).*

Más información en http://creativecommons.org/licenses/by/2.5/es/, o en los datos de contacto indicados.

Contacto
Antonio Villalón Huerta
Director de Seguridad
S2 Grupo

avillalon@s2grupo.es
www.s2grupo.es

Velázquez 150, 2ª planta
28002 Madrid
T.(+34) 902 882 992

Ramiro de Maeztu, 7
46022 Valencia
T.(+34) 902 882 992

Calle 89 nº 12-59
Bogotá (Colombia)
T. (+57) 317 647 10 96

info@s2grupo.es
www.s2grupo.es
www.securityartwork.es