

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

"Gestión de incidentes, tratamiento holístico"



Ruth Sala Ordóñez

Legalconsultors

ruthsala@legalconsultors.es



Amador Aparicio de la Fuente

Salesianos Villamuriel, Talentum Telefónica

amador@centrodonbosco.es

Índice

- 1. Introducción**
- 2. Normativa vinculada a la ciberseguridad**
- 3. Supuestos ciberataques**
- 4. La respuesta de incidentes**
- 5. Modelos preventivos con Hacking Ético y Ciberseguros**

Promulgación de nueva normativa

Directiva NIS

RGPD

Periodo
2015- 2018

Código Penal

L.E.Criminal

Digitalización de los Servicios



Surgen Organizaciones que
proveen de Servicios Esenciales

OBJETIVOS DEL CIBERCRIMEN



“Envenenamiento de software legítimo y otras predicciones de seguridad para 2018”

17 de
noviembre de
2017



Aumentarán el **malware** móvil de alta gama y los hackeos a routers y módems.

Instalación de **mineros** de criptomonedas en las organizaciones

Seguridad industrial ataques dirigidos de **ransomware**

Sector **financiero**, los estafadores intentarán ganar control de las cuentas.

#Ciberseguridad Sujetos Obligados

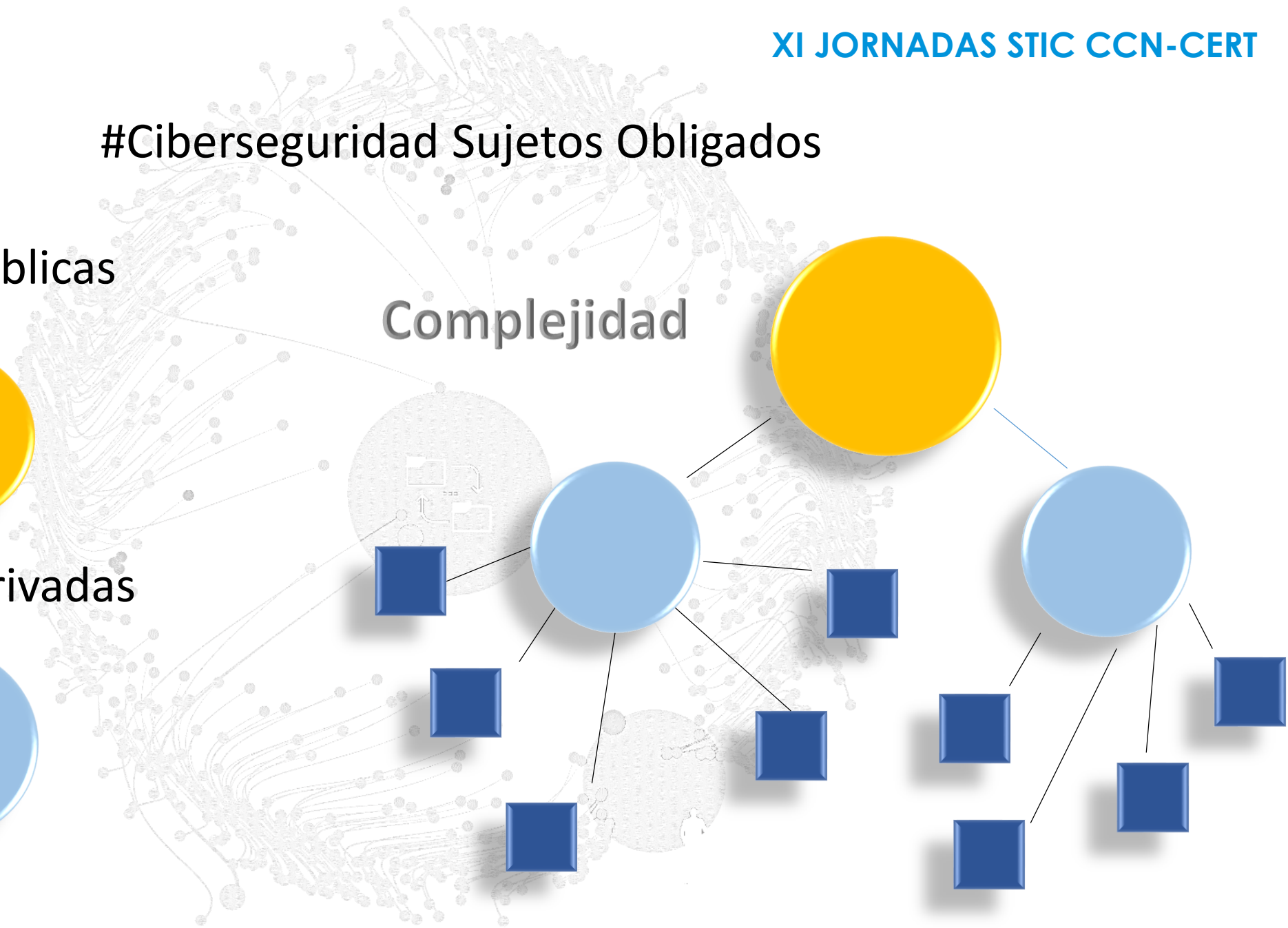
Entidades Públicas



Entidades Privadas



Complejidad



2. Normativa vinculada a la ciberseguridad

Directiva NIS

Mayo 2018

Aplica al
Sector
Público

La transnacionalidad de
la ciberdelincuencia

Falta de homogeneización
en su tratamiento

Servicios
Esenciales

Servicios
Digitales

PROTOCOLOS

ACTUACIÓN

COMUNICACIÓN

DESIGNAR
AUTORIDADES
COMPETENTES

ENISA

Organismo de Coordinación
(Agencia Europea de
Seguridad de las Redes y de
la Información)

**DISPONER DE UNA
ESTRATEGIA
NACIONAL Y**

SEGURIDAD
DE LAS REDES

SISTEMAS DE
INFORMACIÓN

IDENTIFICAR

Operadores de Servicios Esenciales

¿Quién está obligado?



**RELEVANCIA
ANÁLISIS DE
RIESGOS**

Seguridad
de las
Redes

Sistemas de
Información

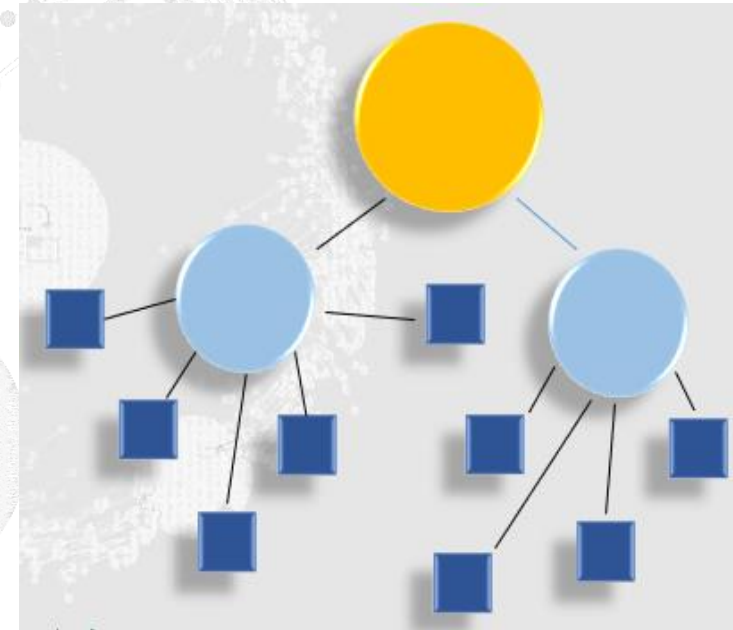


**Fomentar la cultura de
prevención de riesgos**

DIRECTIVA NIS

Plan Nacional de Protección de Infraestructuras Críticas:

“Aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas”



Control de las AA.PP

Servicios
Cloud

Acorde al
ENS

Res.13/10/16 de la Secretaría de Estado Instrucción Técnica de Seguridad de conformidad con el ENS

Requisitos para la **obtención y exhibición** del Certificado de conformidad con el ENS

Confederación Hidrográfica del Guadalquivir

Sistemas **Cloud** / de **Red**

Servicios Digitales que
proveen a Servicios
Esenciales

INCIDENTE

Sanción administrativa

Responsabilidad por daños y perjuicios

¿Responsabilidades penales?

Exigencias

Requisitos de Seguridad
conforme al ENS

Exhibición del
Certificado de
Conformidad
CON EL ENS



Estar conforme al
Reglamento de
Protección de Datos

RGPD

Eficacia 18 mayo 2018

Se introduce el
CIFRADO
ININTELIGIBLE



Determinará el **nivel de medidas de seguridad** técnica necesarias para la protección de la información.



Vinculado a la
CIBERSEGURIDAD



PRIORIDAD

Derechos de los
Individuos



Necesidad de la
EVALUACIÓN DE IMPACTO

Novedades

RGPD

Eficacia 18 mayo 2018

COMUNICACIÓN



USUARIOS

Volumen - Público



PROTOCOLO

ACTUACIÓN COMUNICACIÓN



Organismos de control

CIFRADO



No comunicación

10 millones de euros

2% de la facturación

Sancción



No comunicación

Código Penal

Delitos



Administradores

Alta Dirección

Protocolo de busca de responsabilidades



Sanciones

Personales

Administradores

Multa

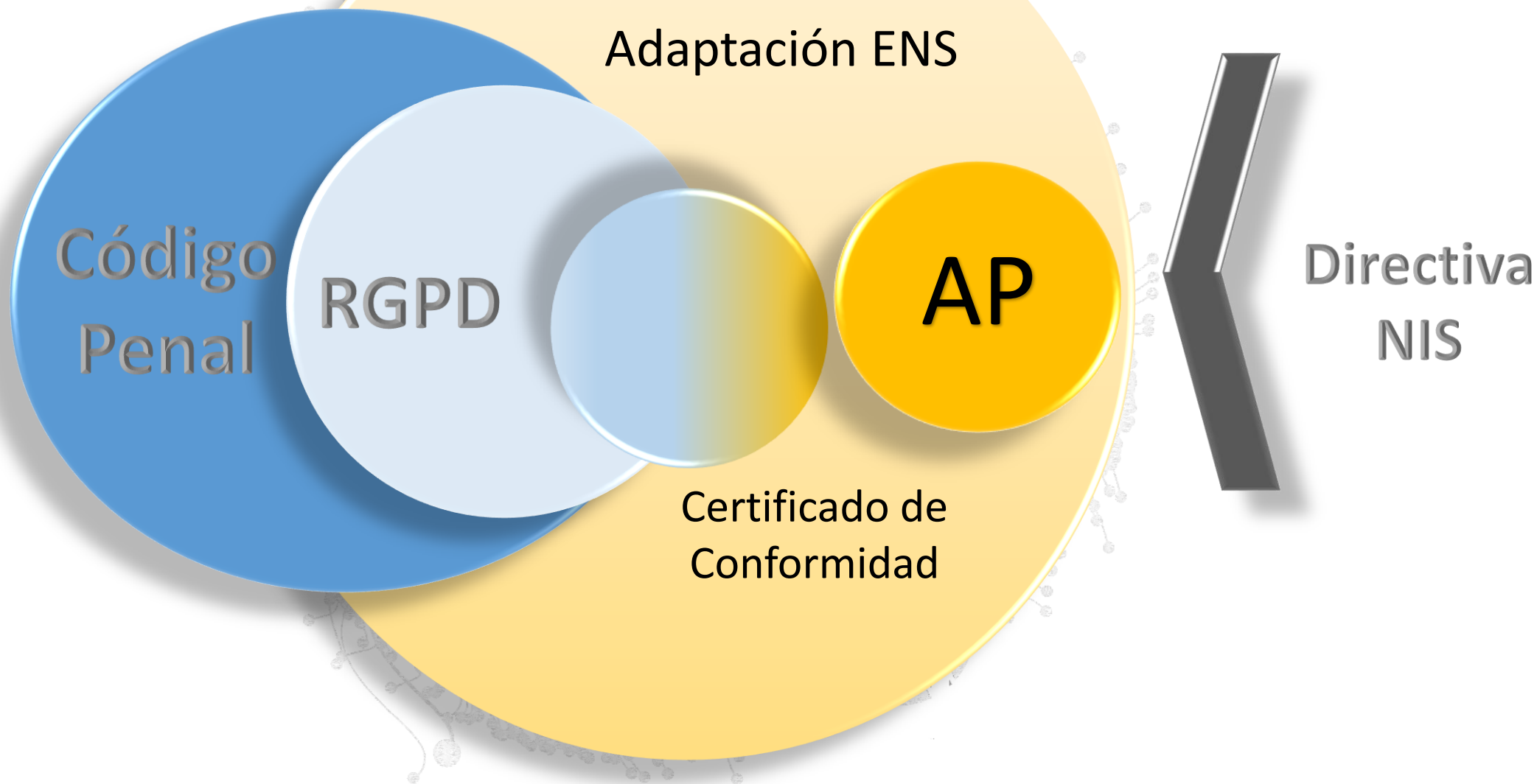
**Cese de Actividad
hasta 5 años**

Artículo 31 bis de
Responsabilidad Penal de
la EMPRESA

¿OBLIGADA?:

PROGRAMA DE
PREVENCIÓN DE
DELITOS

La necesidad de una
Auditoría de Seguridad
del Sistema



Directiva NIS



Código Penal



(Dreamstime.com)



RGPD

impacto

3. “Supuestos” Ciberataques



amador aparicio gasolineras

Todo Maps Imágenes Noticias Vídeos Más Configuración Herramientas

Aproximadamente 21.400 resultados (0,34 segundos)

Gran parte de las gasolineras españolas son vulnerables a ataques ...
www.eldiario.es/.../seguridad-informatica-gasolineras-Espana-hackers_0_371663196....
 1 abr. 2015 - Poco más de veinte minutos necesitó el experto en seguridad informática **Amador Aparicio** para demostrar que muchas **gasolineras** españolas, entre ellas las de algunas de las principales compañías, pueden 'hackearse' de forma alarmantemente sencilla a través de las máquinas que controlan el ...

Amador Aparicio | Perfil profesional - LinkedIn
<https://es.linkedin.com/in/amador-aporicio-007b481>
 Hasta la Cocina en las **Gasolineras** Españolas. securitybydefault.com. marzo de 2015. Inseguridad cibernética en buena parte de las **gasolineras** españolas. Autores: **Amador Aparicio** ...
 Has visitado esta página 5 veces. Fecha de la última visita: 1/10/17.

Accediendo al sistema de control de las gasolineras - Hackpuntos
<https://hackpuntos.com/accediendo-al-sistema-de-control-de-las-gasolineras/>
 29 mar. 2015 - Ayer por la noche estaba leyendo un artículo de **Amador Aparicio** de la Fuente en el que aseguraba que los convertidores de serie a Ethernet del tipo GC-NET2 32-DTE que utilizan las **gasolineras** españolas para controlar los tanques de combustible eran vulnerables (más que vulnerables, mala ...

El grave fallo de seguridad que permite hackear miles de gasolineras
es.gizmodo.com/el-grave-fallo-de-seguridad-que-permite-hackear-miles-d-1699671722
 24 abr. 2015 - El agujero de seguridad lo destapó a finales de marzo **Amador Aparicio**, ingeniero superior en informática y especialista en seguridad. Su hallazgo, detallado por él mismo en un artículo

HASTA LA COCINA DE LAS

Autor: Contribuciones 26 marzo 2015

Muchas gasolineras utilizan túneles serie so estado de los tanques de combustible: tipo c tanque, cantidad de combustible que queda, e

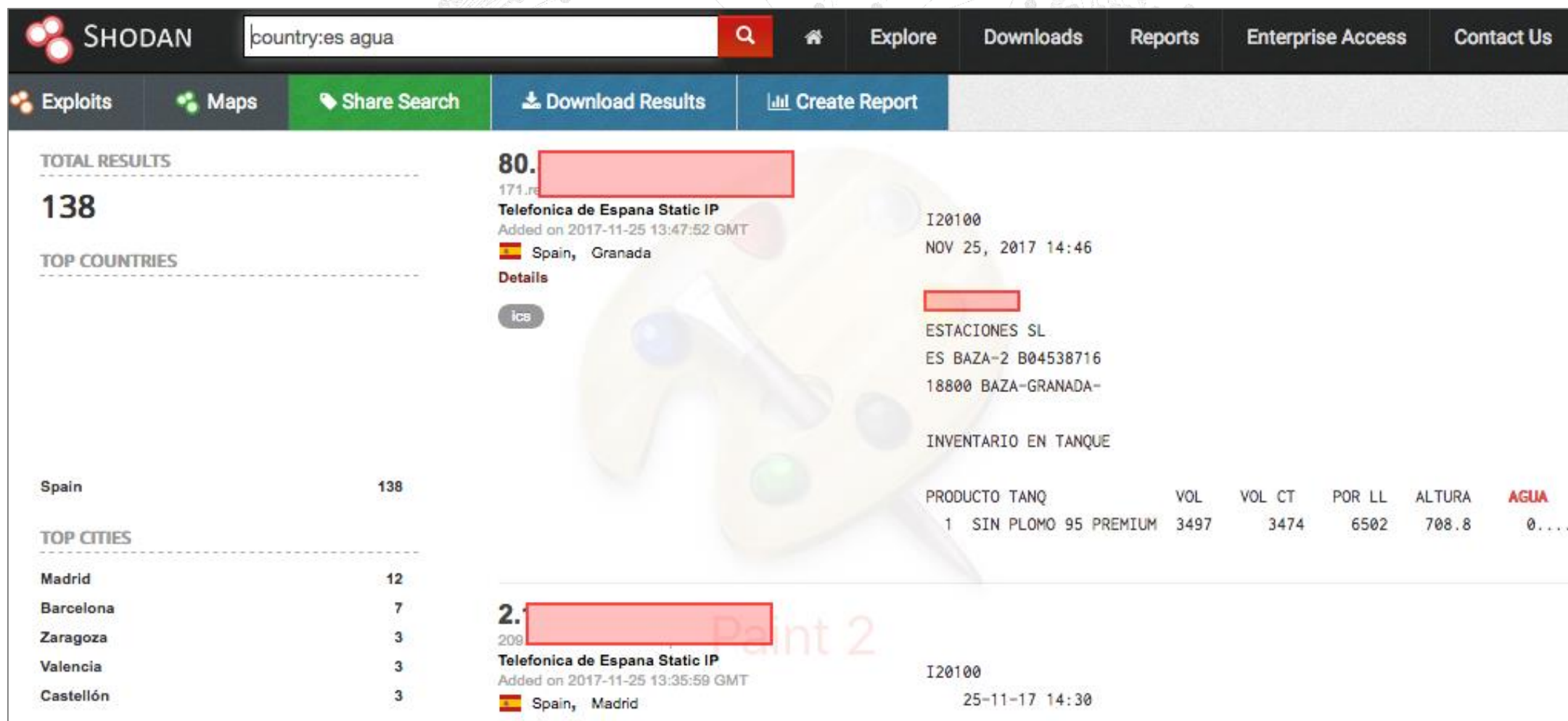
es/tecnologia/noticias/6656994/04/15/De

o informático que
miles de gasolineras

in Share 57 Wow! 0



3. “Supuestos” Ciberataques



SHODAN search results for `country:es agua`.

TOTAL RESULTS
138

TOP COUNTRIES

Country	Count
Spain	138

TOP CITIES

City	Count
Madrid	12
Barcelona	7
Zaragoza	3
Valencia	3
Castellón	3

Results:

80. [Redacted]
171. [Redacted]
Telefonica de Espana Static IP
Added on 2017-11-25 13:47:52 GMT
Spain, Granada
Details
ics

I20100
NOV 25, 2017 14:46

[Redacted]
ESTACIONES SL
ES BAZA-2 B04538716
18800 BAZA-GRANADA-
INVENTARIO EN TANQUE

PRODUCTO	TANQ	VOL	VOL CT	POR LL	ALTURA	AGUA
1	SIN PLOMO 95 PREMIUM	3497	3474	6502	708.8	0....

2. [Redacted]
209 [Redacted]
Telefonica de Espana Static IP
Added on 2017-11-25 13:35:59 GMT
Spain, Madrid

I20100
25-11-17 14:30

3. “Supuestos” Ciberataques

```
MacBook-Pro:~ internet$ telnet 2. [REDACTED] 10001
Trying 2. [REDACTED]
Connected to 209. [REDACTED]
Escape character is '^]'.
^AI20100

I20100
    26-11-17 11:52

C.T NAVALMORAL

INVENTARIO EN TANQUE

PRODUCTO TANQ          VOL    VOL CT    POR LL
 1  GASOLEO A          13376    13338    25667
```

HIST ALARMAS TANQS

TANQ 1 GASOLEO C

ALARM BAJA PRODUCTO	23-11-17 11:29
	16-11-17 10:45
	09-11-17 13:43
CARGA NECESITADA	23-11-17 11:27
	16-11-17 10:13
	09-11-17 13:42

TANQ 2 GASOLEO B2

ALARMA AJUSTE DATOS	18-01-17 16:03
ALARMA SOBRECARGA	25-01-17 9:05
ALARM BAJA PRODUCTO	20-11-17 8:04
	06-11-17 13:35
	06-11-17 8:59
ALARM ALTA PRODUCTO	25-01-17 9:00
	18-01-17 16:03
CARGA NECESITADA	20-11-17 8:03
	06-11-17 13:34
	06-11-17 8:58

3. “Supuestos” Ciberataques

Wireshark · Follow TCP Stream (tcp.stream eq 533) · wireshark_en1_20171126155947_2HjgyX

.I20100
.
I20100
26-11-17 16:43

C.T NAVALMORAL

INVENTARIO EN TANQUE

PRODUCTO	TANQ	VOL	VOL CT	POR LL	ALTURA	AGUA	TEMP
1	GASOLEO A	13202	13160	25841	923.1	0.0	19.02

..

3. “Supuestos” Ciberataques

The Communications Interface supports the following TLS-350 display format commands:

Table 3. TLS-350 Display Format Commands

Commands
S00100 Reset
S00200 Clear Reset Flag
S00300 Remote Alarm Reset
I10100 System Status Report
I20100 Inventory
I20200 Delivery
I20400 Shift Inventory
I20500 Tank Status
I20600 Tank Alarm History
I30100 Sensor Status
I30200 Sensor Alarm History
I40600 Relay Status
S50100 Set Time of Day
IA0100 Tank Diagnostics
IB0100 Sensor Diagnostics

Google

I20100 ext:pdf root

Todo

Maps

Videos

Imágenes

Aproximadamente 6.080 resultados (0,37

[PDF] Guardian - Veeder-Root

www.veeder.com/gold/download.cfm?

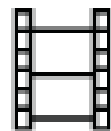
22 sept. 1994 - Printer Interface. The printer interface allows the user to perform the following commands: S00100 Reset. S00200 Clear Reset Flag. S00300 Remote Alarm Reset. I10100 System Status Report. I20100 Inventory. I20200 Delivery. I20400 Shift Inventory. I20500 Tank Status. I20600 Tank Alarm History. I30100 Sensor Status. I30200 Sensor Alarm History. I40600 Relay Status. S50100 Set Time of Day. IA0100 Tank Diagnostics. IB0100 Sensor Diagnostics.

Has visitado esta página 3 veces. Fecha

3. “Supuestos” Ciberataques

- **Sistemas no securizados.**
- **Protocolos inseguros.**
- **¿Infraestructura Crítica?**
- **¿Responsabilidad del fabricante?**
- **¿Capacidad de localizar todos estos sistemas de un país?**
- **¿Una vez localizados?**

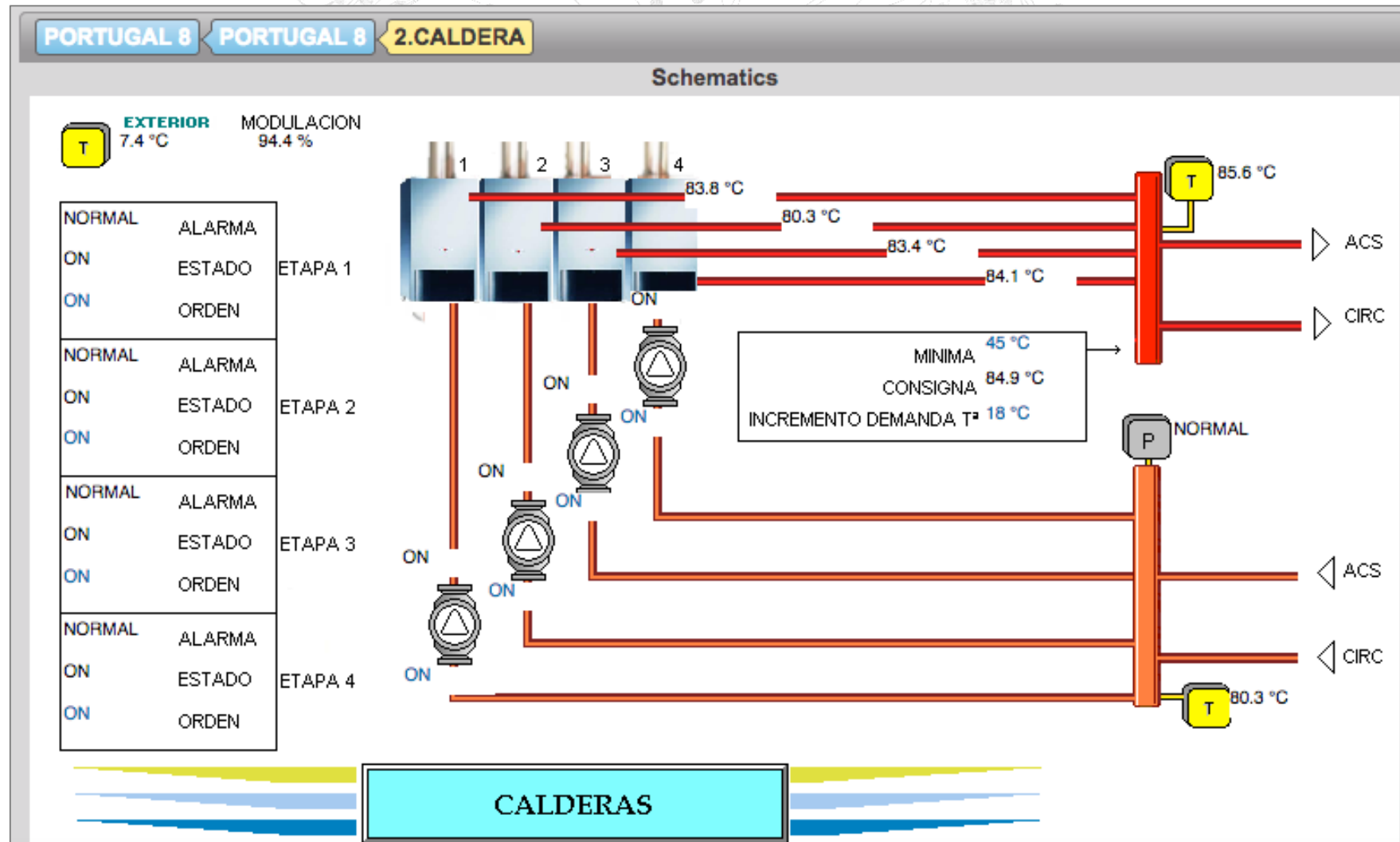
3. “Supuestos” Ciberataques



Sistema Control Tanques de Combustible

DEC 13, 2017

3. “Supuestos” Ciberataques



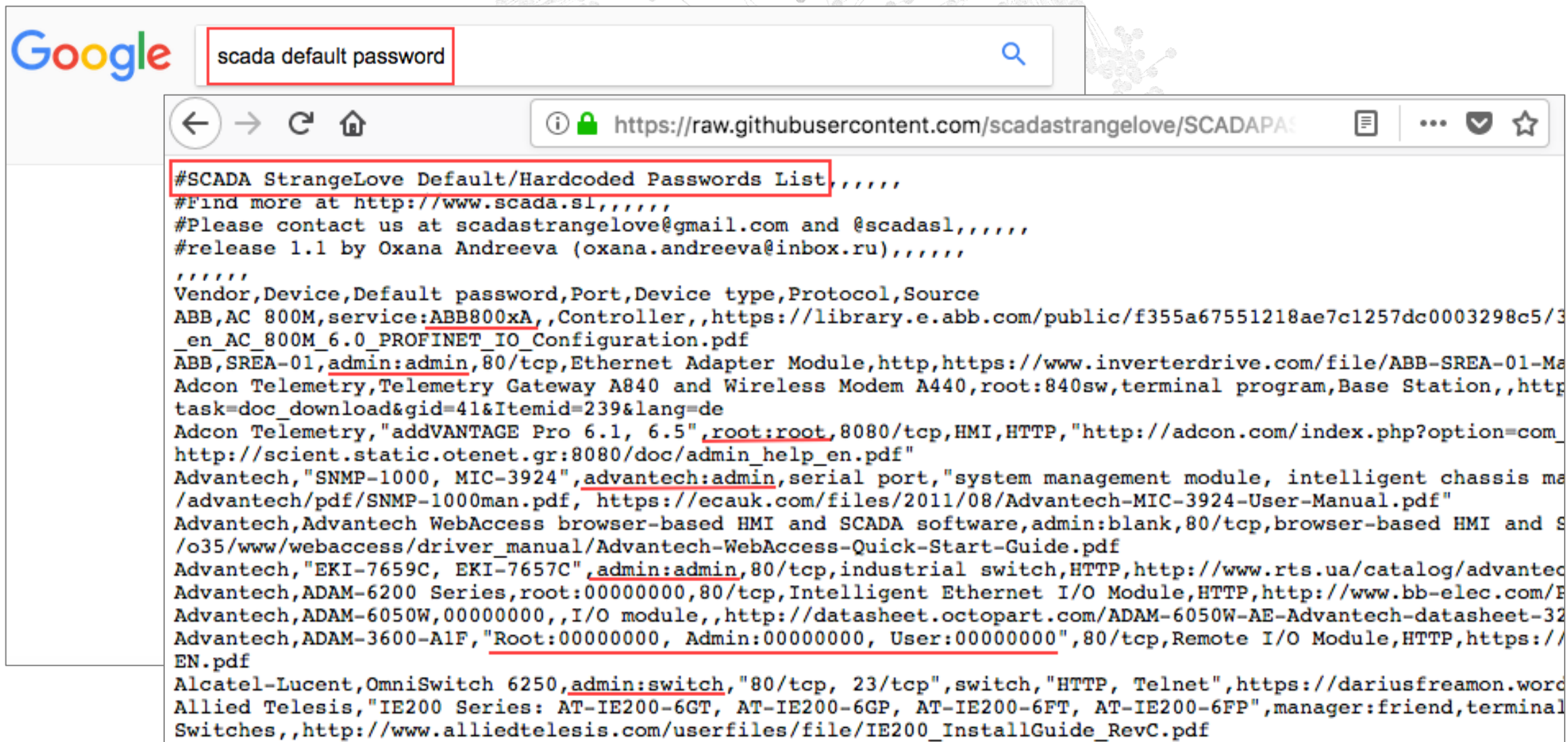
3. “Supuestos” Ciberataques

http.request.method=="POST"

No.	Time	Source	Destination	Protocol	Length	Info
29	16.486725	192.168.1.7	81. [REDACTED]	HTTP	632	POST /login HTTP/1.1

- ▶ Frame 29: 632 bytes on wire (5056 bits), 632 bytes captured (5056 bits) on interface 0
- ▶ Ethernet II, Src: Apple_d0:df:e8 (20:3c:ae:d0:df:e8), Dst: [REDACTED] 7c:59:cc)
- ▶ Internet Protocol Version 4, Src: 192.168.1.7, Dst: 81. [REDACTED]
- ▶ Transmission Control Protocol, Src Port: 53136, Dst Port: 8080, Seq: 1, Ack: 1, Len: 566
- ▶ Hypertext Transfer Protocol
- ▼ HTML Form URL Encoded: application/x-www-form-urlencoded
 - ▶ Form item: "locale" = "es"
 - ▶ Form item: "login" = "admin"
 - ▶ Form item: "password" = "passwd"
 - ▼ Form item: "submit" = "Inicio de sesión"

3. “Supuestos” Ciberataques



The image shows a Google search for "scada default password" and a browser window displaying a list of SCADA default passwords from a GitHub repository. The search results are highlighted in red. The browser window shows the raw content of a GitHub file, which is a list of SCADA devices and their default passwords. The list includes entries for ABB, Advantech, Alcatel-Lucent, and Allied Telesis, among others. The passwords are listed in a structured format, including vendor, device, default password, port, device type, protocol, and source.

Google search results for "scada default password":

- #SCADA StrangeLove Default/Hardcoded Passwords List,,,,,
- #Find more at <http://www.scada.sl>,,,,,
- #Please contact us at scadastrangelove@gmail.com and @scadasl,,,,,
- #release 1.1 by Oxana Andreeva (oxana.andreeva@inbox.ru),,,,,,

Browser window content (raw.githubusercontent.com/scadastrangelove/SCADAPAS):

```
Vendor,Device,Default password,Port,Device type,Protocol,Source
ABB,AC 800M,service:ABB800xA,,Controller,,https://library.e.abb.com/public/f355a67551218ae7c1257dc0003298c5/3_en_AC_800M_6.0_PROFINET_IO_Configuration.pdf
ABB,SREA-01,admin:admin,80/tcp,Ethernet Adapter Module,http,https://www.inverterdrive.com/file/ABB-SREA-01-Ma
Adcon Telemetry,Telemetry Gateway A840 and Wireless Modem A440,root:840sw,terminal program,Base Station,,http
task=doc_download&gid=41&Itemid=239&lang=de
Adcon Telemetry,"addVANTAGE Pro 6.1, 6.5",root:root,8080/tcp,HMI,HTTP,"http://adcon.com/index.php?option=com_
http://scient.static.otenet.gr:8080/doc/admin_help_en.pdf"
Advantech,"SNMP-1000, MIC-3924",advantech:admin,serial port,"system management module, intelligent chassis ma
/advantech/pdf/SNMP-1000man.pdf, https://ecauk.com/files/2011/08/Advantech-MIC-3924-User-Manual.pdf"
Advantech,Advantech WebAccess browser-based HMI and SCADA software,admin:blank,80/tcp,browser-based HMI and S
/o35/www/webaccess/driver_manual/Advantech-WebAccess-Quick-Start-Guide.pdf
Advantech,"EKI-7659C, EKI-7657C",admin:admin,80/tcp,industrial switch,HTTP,http://www.rts.ua/catalog/advantec
Advantech,ADAM-6200 Series,root:00000000,80/tcp,Intelligent Ethernet I/O Module,HTTP,http://www.bb-elec.com/E
Advantech,ADAM-6050W,00000000,,I/O module,,http://datasheet.octopart.com/ADAM-6050W-AE-Advantech-datasheet-32
Advantech,ADAM-3600-A1F,"Root:00000000, Admin:00000000, User:00000000",80/tcp,Remote I/O Module,HTTP,https://
EN.pdf
Alcatel-Lucent,OmniSwitch 6250,admin:switch,"80/tcp, 23/tcp",switch,"HTTP, Telnet",https://dariusfreamon.word
Allied Telesis,"IE200 Series: AT-IE200-6GT, AT-IE200-6GP, AT-IE200-6FT, AT-IE200-6FP",manager:friend,terminal
Switches,,http://www.alliedtelesis.com/userfiles/file/IE200_InstallGuide_RevC.pdf
```

3. “Supuestos” Ciberataques

The image shows a web application interface for configuring an email server. The interface is divided into two main sections: "Servidor e-mail" and "Formato de e-mail (notificación)". The "Servidor e-mail" section contains a "Configuración del servidor de e-mail" tab, which is currently selected. This tab displays the "Configuración de servidor de correo" settings, including the SMTP server, port, sender email, username, password, and SSL status. The "Formato de e-mail (notificación)" section is also visible but not selected.

Overlaid on the right side of the interface is a browser's developer tools window, specifically the "Inspector" tab. It shows the HTML structure of the password field, which is highlighted in blue. The HTML code for the password field is as follows:

```
<tr>
  <td class="mark_individual" colspan="2">Contraseña</td>
  <td class="quitation" colspan="2">
    <input id="passwordmail" class="input" name="passwordmail" value="n[REDACTED]5"
      autocomplete="off" size="40" type="password">
  </td>
</tr>
```

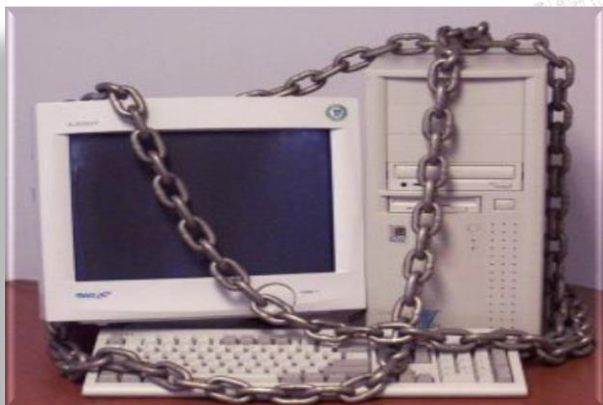
3. “Supuestos” Ciberataques



3. “Supuestos” Ciberataques

- **Sistemas no securizados.**
- **Protocolos inseguros.**
- **¿Infraestructura Crítica?**
- **¿Responsabilidad del fabricante?**
- **¿Capacidad de localizar todos estos sistemas de un país?**
- **¿Una vez localizados?**

Respuesta de incidentes



Protocolos de respuesta de incidencias

¿Por dónde
empezar?



**Test Sistema de
Información**



Medidas

Disponibilidad

Sensibilidad

Autenticidad

Confidencialidad



Calidad

Integridad

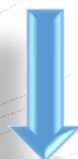
Protección

Elemento Común a toda la normativa:

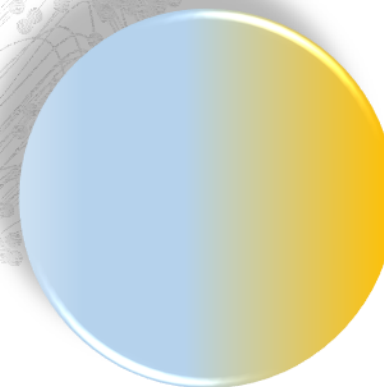
Código Penal



Directiva NIS



RGPD



Código Penal

Establecer los roles
internos y formación
para la prevención de
delitos

Especial atención a los
proveedores de
servicios tecnológicos

OBJETIVO

Ganar la **EXIMENTE**

Directiva NIS

Protocolos de actuación en
caso de **incidentes**

RGPD

Regulación del
tratamiento de
la Información

Cifrado de la
Información

OBJETIVO

EVITAR SANCIÓN administrativa
+ INDEMNIZACIONES

Evaluación de



**Seguridad
Defensiva**

**Seguridad
Ofensiva**

Modalidades de Hacking

White Box

Se conoce el funcionamiento interno de la aplicación

Grey Box

Se conoce parcialmente el funcionamiento interno

Black Box

No se conoce nada de la aplicación ni del sistema

Daños propios

Ransomware – Ataque DDOS
– Daños en Hardware y Software – Ciberextorsión – Restauración del sistema tras un ataque

Payment Card Industry

Gastos de Defensa

Fianzas y sanciones o multas regulatorias

Gastos de Auditoría y Forense



Responsabilidad Civil

Filtración o Pérdida de Datos

Violaciones de Privacidad

Violación de derechos de PI e Industrial

Pérdida o robo de activos digitales con información confidencial

Daños por intervención en medios digitales

Malware con propagación externa

Gracias



Ruth Sala Ordóñez

Legalconsultors

ruthsala@legalconsultors.es

Gestión de Incidentes, “tratamiento holístico”



Amador Aparicio de la Fuente

Salesianos Villamuriel

amador@centrodonbosco.es

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

