

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

"Habías Tenido Tiempo Para Securizarlo..." (HTTPS)

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

**"Has Tenido Tiempo Para Securizarlo: Te Lo Suplico,
no Sigas Sólo Leyendo" (HTTPS: TLS, no SSL)**

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

**"Habías Tenido Tiempo Para Securizarlo: Te Lo
Supliqué, no Sigas Siendo Lerdo"
(HTTPS: TLS, no SSL)**

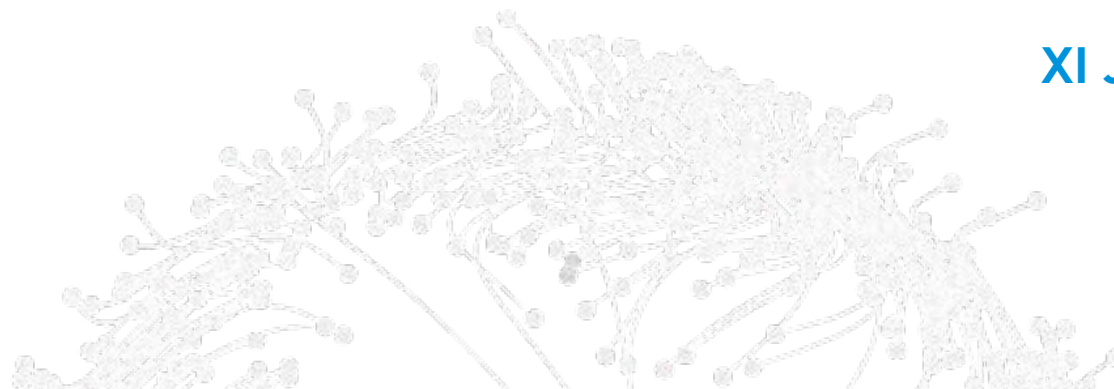
XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

**"Habías Tenido Tiempo Para Securizarlo: Te Lo
Supliqué, no Sigas Siendo Lerdo"**
(HTTPS: TLS, no SSL)



lerdo, da

Etim. disc.

1. adj. Dicho comúnmente de una bestia: Pesada y torpe en el andar.
2. adj. Tardo y ~~torpe~~ para comprender o ejecutar algo.
3. f. Veter. Tumor de las caballerías cerca de la rodilla.

Real Academia Española © Todos los derechos reservados



§ DinoSec



- Raúl Siles
- DinoSec (www.dinosec.com)
- raul@dinosec.com

Índice

1. **Actividades previas (2016-2017) y recursos de ayuda**
2. **Selección de objetivos**
3. **Tipos de análisis realizados**
4. **Resultados del estudio piloto**
5. **Resultados de la fase 1 del estudio completo**
6. **Resultados de la fase 2 del estudio completo**
7. **Conclusiones**

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Actividades previas (2016-2017) y recursos de ayuda

Actividades previas (2016-2017) y recursos de ayuda (1/4)

- X Jornadas (diciembre 2016)
 - "Has Tenido Tiempo Para Securizarlo: Te Lo Suplico, no Sigas Solo Leyéndolo" (concienciación y documentación)
 - <https://www.ccn-cert.cni.es/xjornadas> (presentación + vídeo)
 - CONAND (febrero 2017): Andorra
- Estudio HTTPS piloto (febrero 2017)
 - Plazo de recepción de objetivos: enero 2017
 - Resultados y "entrega de informes": VII Jornadas SAT
- VII Jornadas SAT (9 marzo 2017)
 - "Implementación HTTPS sedes electrónicas Sector Público" (resultados estudio piloto)
 - <https://www.ccn-cert.cni.es/gestion-de-incidentes-2/sistema-de-alerta-temprana-sat/jornada-sat/vii-jornada-sat.html> (necesario registro)

Actividades previas (2016-2017) y recursos de ayuda (2/4)

- Guía de Buenas Prácticas (abril 2017)
 - "Buenas Prácticas CCN-CERT BP-01/17: Recomendaciones de implementación de HTTPS" (ZIP = PDF + Excel)
 - <https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp.html>
 - Fichero ZIP: <https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/2109-ccn-cert-bp-01-17-recomendaciones-implementacion-https/file.html>
- Curso de formación online (finales de julio 2017 – 2 sesiones)
 - VANESA: <https://vanesa.ccn-cert.cni.es>
 - "Recomendaciones Implementación HTTPS" (vídeo: 3 horas)

Actividades previas (2016-2017) y recursos de ayuda (3/4)

- Estudio HTTPS completo: Fase 1 (julio 2017)
 - Plazo de recepción de objetivos: 19 de mayo & 24 de mayo (Wannacry)
 - <https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4455-analisis-de-la-implementacion-https-de-entornos-y-aplicaciones-web-en-el-sector-publico.html>
 - <https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/4515-ampliado-el-plazo-de-solicitud-del-analisis-de-implementacion-https-en-entornos-web-del-sector-publico.html>
 - Resultados: **"HOY"**
 - "Resumen Ejecutivo CCN-CERT: Resultados del estudio de la implementación de HTTPS en el Sector Público – Organismo X" (septiembre 2017)
 - Informe + Ficheros Excel y CSV, junto a ficheros de log y depuración
 - "Informe Técnico CCN-CERT: Interpretación de los resultados del estudio de la implementación de HTTPS en el Sector Público"
 - Entrega de informes: principios de octubre 2017
 - <https://www.ccn-cert.cni.es/seguridad-al-dia/comunicados-ccn-cert/5143-mas-de-225-organismos-participan-en-la-primera-fase-del-estudio-de-implementacion-de-https-en-el-sector-publico.html>

Actividades previas (2016-2017) y recursos de ayuda (4/4)

- Estudio HTTPS completo: Fase 2 (noviembre 2017)
 - Plazo de recepción de objetivos: 31 de octubre de 2017
 - Cambios y modificaciones, y nuevos organismos y dominios
 - Resultados: **HOY**
 - Entrega de informes: diciembre 2017 / enero 2018
- E-mail: **estudioHTTPS@ccn-cert.cni.es**

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Selección de objetivos

Selección de objetivos (1/2)

- Alcance: Sector Público
 - Desde grandes organismos y ministerios, hasta pequeños ayuntamientos
 - AGE, CCAA, Entidades locales, Universidades, Organismos constitucionales...
- Fichero Excel para la selección de objetivos
 - Objetivo: Automatización del análisis
 - Excel, Python, bash, PowerShell, Word, etc.
 - Requisitos y recomendaciones
 - Guía de BP – Anexo A, y fichero Excel
 - "Se deben de leer todas las instrucciones detalladamente..."



Selección de objetivos (2/2)

- Problemáticas
 - Objetivos disponibles públicamente en Internet
 - Imposibilidad de analizar objetivos privados (ej. red SARA)
 - Objetivos relevantes identificados por su nombre (o "hostname")
 - Imposibilidad de usar direcciones IP (certificados digitales públicos)
 - Objetivos: dominio y www
 - Ejemplo: www.ccn-cert.cni.es
 - No incluir el dominio principal como objetivo (por ejemplo, "cni.es").
 - No incluir el protocolo (por ejemplo, "http://..." o "https://...").
 - No incluir recursos concretos (por ejemplo, "www.ccn-cert.cni.es/cursos/").
 - Puertos TCP/80 y TCP/443 (otros puertos no estándar no incluídos)
 - Disponibilidad: DNS, IPv4 vs. IPv6, servicios web, etc.
 - Limitaciones si el obligatorio el uso de certificado digital cliente



Microsoft
Excel Worksheet

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Tipos de análisis realizados

Tipos de análisis realizados

- Nmap
 - Analizar el estado de los puertos TCP/IP: TCP/80 (HTTP) y TCP/443 (HTTPS)
- pshtt
 - Obtener una visión general de la implementación de HTTPS
 - Evaluar la importancia y prioridad que se le otorga a HTTPS frente a HTTP
- SSL Labs
 - Obtener una visión global y muy detallada de la implementación de HTTPS
 - Analizar múltiples aspectos de HTTPS que permiten evaluar en profundidad la configuración de HTTPS en el entorno web objetivo

Nmap

Resultados esperados: estado de los puertos TCP/IP

- Puerto TCP/443 abierto
 - ¿Puerto TCP/443 filtrado o cerrado?
- Puerto TCP/80 abierto (con redirección hacia TCP/443), cerrado o filtrado

Resultados esperados: visión general de la implementación de HTTPS

- Soporte de HTTPS adecuado
 - Dominio y servidor web (www): http:// y https://
 - Validez del certificado digital: cadena de certificados digitales (CAs), hostname, y expiración
- Prioridad de HTTPS frente a HTTP
 - Redirección de HTTP a HTTPS (y no al revés: *downgrade*)
- Prioridad de HSTS
 - HSTS robusto: periodo de validez ($\text{max-age} \geq 1$ año), aplicación a todo el dominio, preload (ya incluido o pendiente)....

pshtt (calificación)

Calificación: visión general de la implementación de HTTPS

- Clasificación en base a cuatro niveles o grados de cumplimiento
 - Cumplimiento **bajo** (<5).
 - Cumplimiento **medio** (≥ 5 y <7.5).
 - Cumplimiento **alto** (≥ 7.5 y <9).
 - Cumplimiento **excelente** (≥ 9).

Domain Supports HTTPS	Domain Enforces HTTPS	Domain Uses Strong HSTS
TRUE	TRUE	TRUE

SSL Labs

Resultados esperados: visión global y detallada de la implementación de HTTPS

- Qualys SSL Labs: SSL Server Test (APIs)
 - <https://www.ssllabs.com/ssltest/>
- Protocolos SSL/TLS, validez del certificado, HSTS (implementado correctamente), HPKP (Report-Only), OCSP Stapling, etc.
- Calificación (o *grade*) empleando el sistema de calificación americano, basado en letras (personalizado en cuatro niveles)
- **¿SSL Labs: Grade?**
- HPKP o HPKP-RO (¿desechado por la industria en 2017?)

SSL Labs (calificación)

Calificación: visión global y detallada de la implementación de HTTPS

- Clasificación en base a cuatro niveles o grados de cumplimiento

Table 1. Letter grade translation

Numerical Score	Grade
score $\geq$ 80	A
score $\geq$ 65	B
score $\geq$ 50	C
score $\geq$ 35	D
score $\geq$ 20	E
score $<$ 20	F

- Cumplimiento **bajo**: C-F.

- F (2)

- E (3)

- D (4)

- C (5)

- Cumplimiento **medio**: B (7).

- Cumplimiento **alto**: A (9) y A- (8).

- Cumplimiento **excelente**: A+ (10).

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Resultados del estudio piloto

Resultados del estudio piloto

Objetivos

- Objetivos potenciales recibidos
 - 26 Ministerios, Organismos, Agencias, CCAA, etc.
 - +200 objetivos (selección de 1 ó 2 por organismo)
- Objetivos: 46
 - Puertos TCP/IP: 45 (46-1)
 - 1 objetivo no disponible en DNS
 - Análisis HTTPS: 44 (46-1-1)
 - 1 objetivo no alcanzable en TCP/80 o TCP/443
 - SSL Labs: 39 (46-1-6)
 - 3 objetivos tienen TCP/443 filtrado, 2 objetivos no pueden ser analizados por SSL Labs (bugs), 1 objetivo identificado por dirección IP

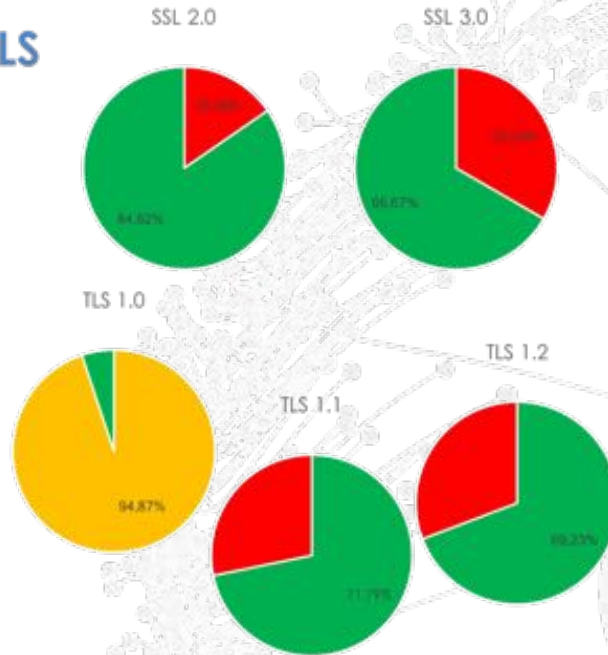
Resultados del estudio piloto (1/2)

Nmap, pshtt y SSL Labs

- Puertos TCP/IP (45)
 - TCP/80: Filtrado en 7 y cerrado en 1 (18,6%)
 - TCP/443: ¿Filtrado en 3 (7%)?
- Análisis HTTPS (44)
 - No hay redirección de HTTP a HTTPS: 43%
 - Hay redirección de HTTPS a HTTP (*downgrade*): 6,82%
 - Uso correcto de HTTPS (aproximadamente): 50%
- SSL Labs (39)
 - HSTS: 6,82%
 - ...

Protocolos SSL/TLS

- SSL 2.0: **15,38%**
- SSL 3.0: **33,33%**
- TLS 1.0: **94,87%**
- TLS 1.1: **71,79%**
- TLS 1.2: **69,23%**



Resultados del estudio piloto (2/2)

SSL Labs: Score

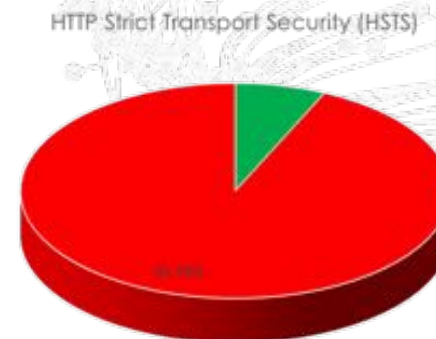
- A+, A, A-: **33,33%**
- B, C, D: **43,59%**
- E, F: **23,08%**



Score	Porcentaje
A+	0,00%
A	15,38%
A-	2,56%
B	12,82%
C	10,26%
D	0,00%
E	0,00%
F	23,08%
T	35,90%

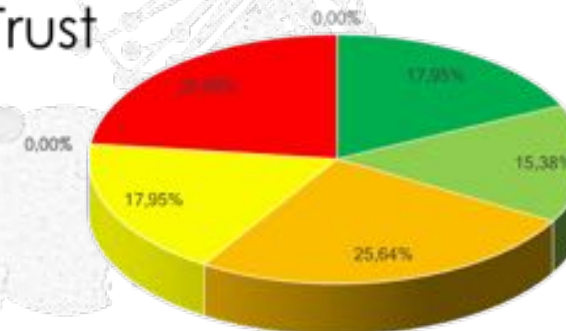
HTTPS Strict Transport Security (HSTS o STS)

- Utilizado por: **6,82% (3/44)**
 - includeSubDomains: **100%**
 - max-age:
 - 365 días (1 año)
 - 72 horas (3 días)
 - "500" (8,3 minutos) ☹
 - preload: **0%**
 - Preload pending: **0%**



- T: No Trust

SSL Labs: Score/Grade



Score	Porcentaje
A+	0,00%
A	17,95%
A-	15,38%
B	25,64%
C	17,95%
D	0,00%
E	0,00%
F	23,08%
T	0,00%

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Resultados de la fase 1 del estudio completo

Objetivo: Facilitar la correcta implementación de HTTPS

- Para todos los estudios realizados: piloto, fase 1 y fase 2
- Desde el anuncio inicial y el periodo de recepción de objetivos, hasta el momento del análisis, se dejaron pasar unas semanas
 - **Para no "pillar" a nadie desprevenido 😊**
 - Comunicaciones del tipo: "...¿hay alguien ahí?" 😊

Resultados de la fase 1 del estudio completo

Objetivos

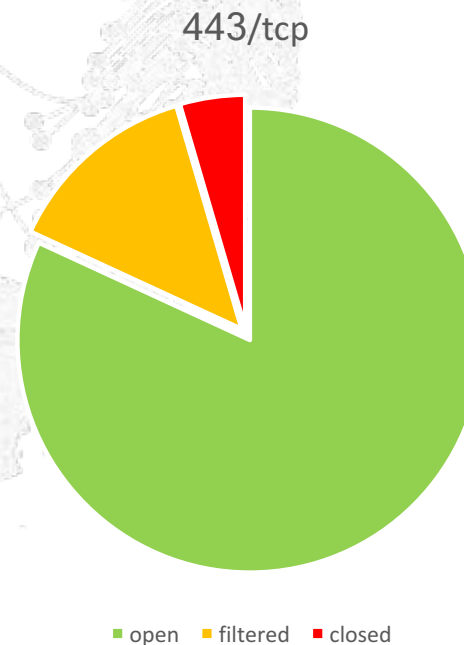
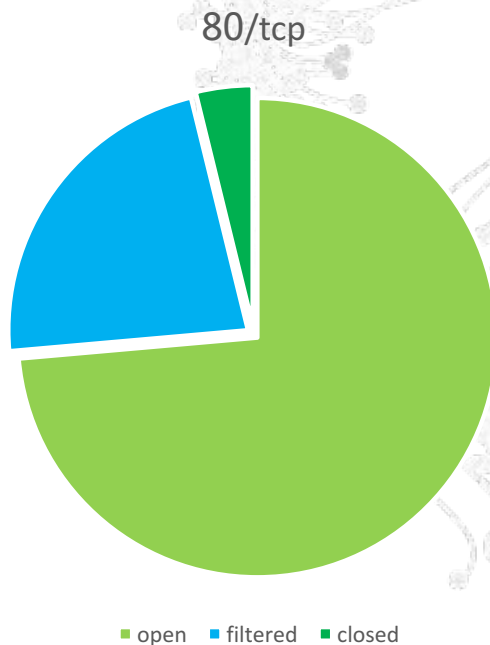
- Organismos: 227
- Dominios: 635
- Hostnames: 3.537



Resultados de la fase 1 del estudio completo

Nmap

- Total puertos TCP (x2): 2.273
- TCP/80: Filtrado en 513 y cerrado en 87 (26,40%)
- TCP/443: ¿Filtrado en 309 y cerrado en 103 (18,13%)?



Resultados de la fase 1 del estudio completo

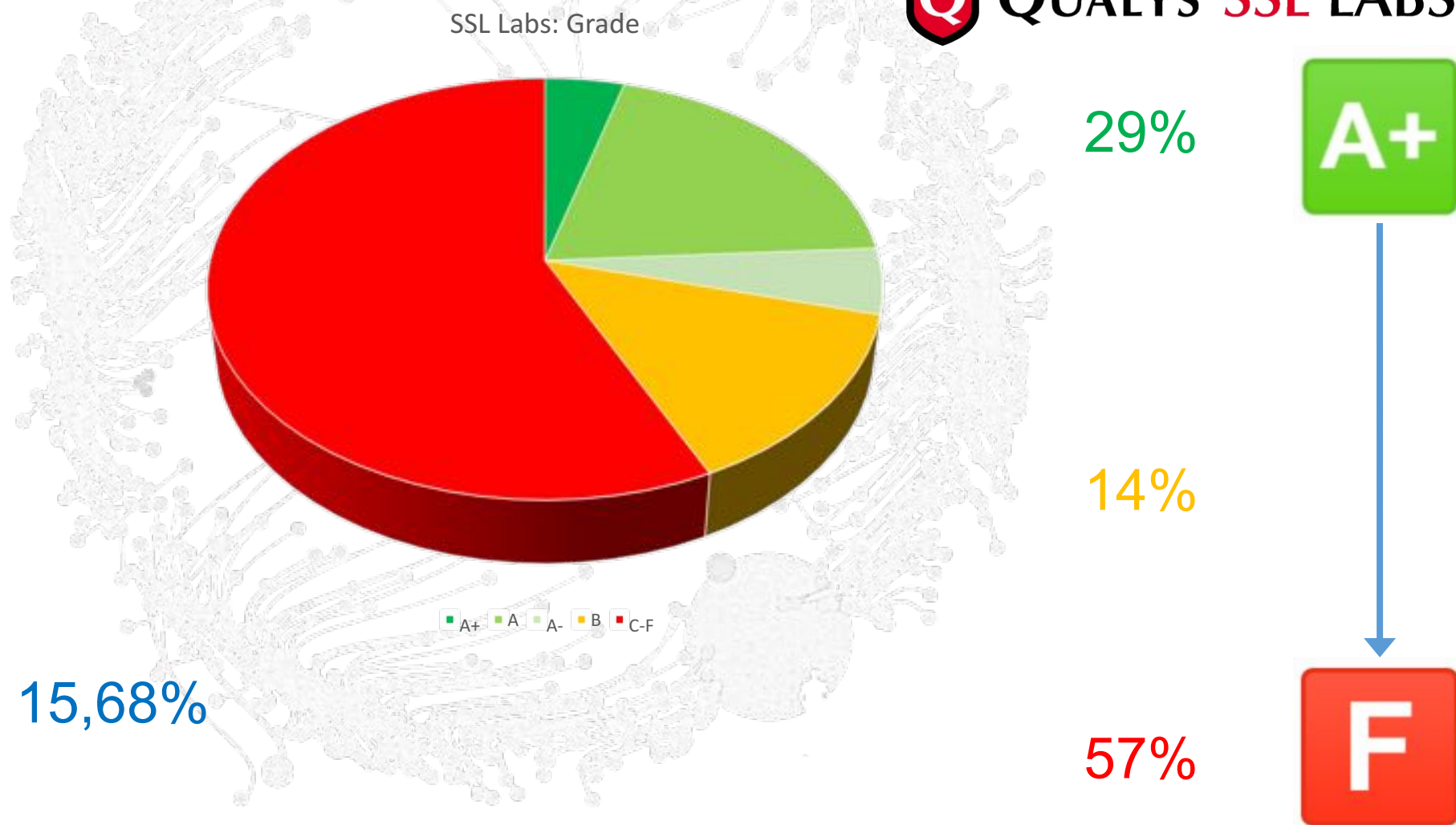
pshtt

- Total: 3728
- Dominio soporta HTTPS: 39,65%
 - Hostname incorrecto en certificado: 13,01%
 - Certificado expirado o cadena no válida: 0%
- Dominio prioriza HTTPS: 26,05%
 - HTTPS downgrades: 2,84%
- Dominio usa HSTS robusto: 3,76%
 - HSTS: 5,07% (para todo el dominio: 3,03%)
 - Listo para preload: 1,37% (dominio precargado: 0%)

Resultados de la fase 1 del estudio completo

SSL Labs

- Total: 2.595
- A+: 4,32%
- A: 19,73%
- A-: 5,05%
- B: 13,80%
- C-F: 57,11%
- T (No Trust): 15,68%



XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Resultados de la fase 2 del estudio completo

Resultados de la fase 2 del estudio completo

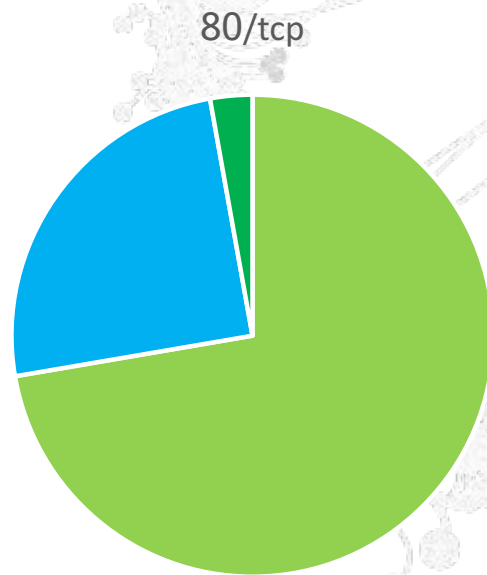
Objetivos

- Organismos: 249 (+22)
- Dominios: 683 (+48)
- Hostnames: 3.794 (+257)
- Modificaciones respecto a la fase 1:
 - Actualizaciones de organismos: 12
 - Nuevos organismos: 22

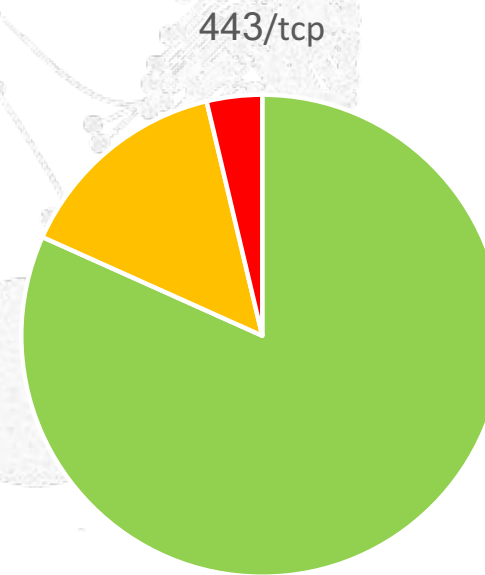
Resultados de la fase 2 del estudio completo

Nmap

- Total puertos TCP (x2): 2.477 (+204)
- TCP/80: Filtrado en 616 y cerrado en 70 (27,69%)
- TCP/443: ¿Filtrado en 361 y cerrado en 92 (18,29%)?



■ open ■ filtered ■ closed



■ open ■ filtered ■ closed

Resultados de la fase 2 del estudio completo

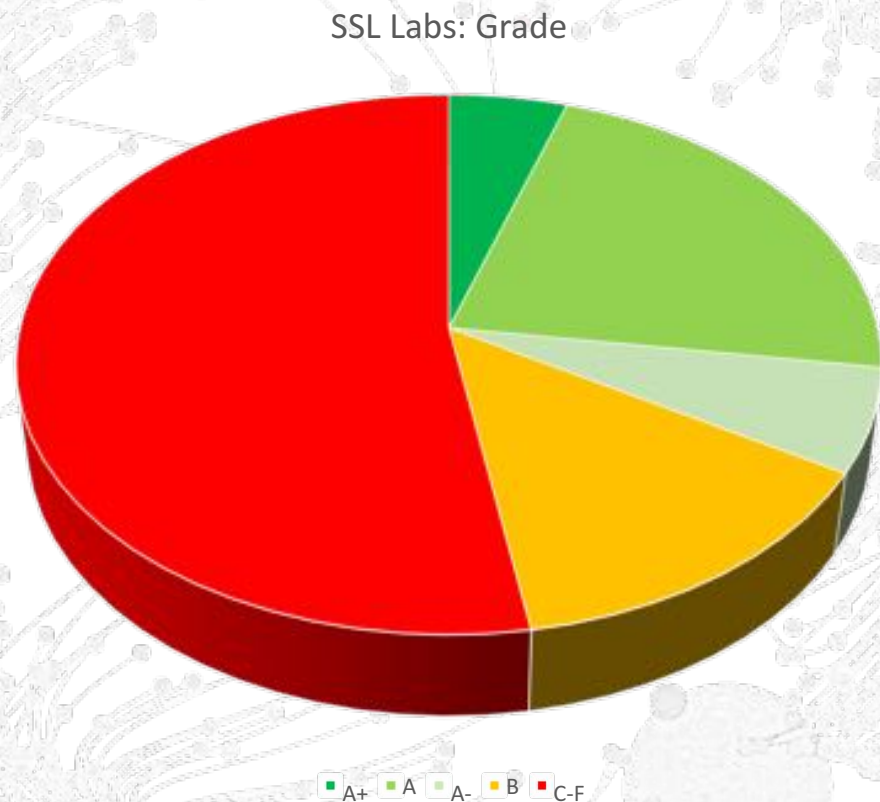
pshtt

- Total: 3941 (+213)
- Dominio soporta HTTPS: 40,83% (+1%)
 - Hostname incorrecto en certificado: 16,11% (+3%)
 - Certificado expirado o cadena no válida: 0% (=)
- Dominio prioriza HTTPS: 29,18% (+3%)
 - HTTPS downgrades: 2,84% (=)
- Dominio usa HSTS robusto: 4,21% (+0,5%)
 - HSTS: 5,51% (para todo el dominio: 3,50%)
 - Listo para preload: 1,57% (dominio precargado: 0,05%)

Resultados de la fase 2 del estudio completo

SSL Labs

- Total: 2.595 (+229)
- A+: 5,03%
- A: 22,31%
- A-: 6,20%
- B: 13,81%
- C-F: 52,66%
- T (No Trust): 16,04%



33,5%
(+4,5%)



14%

52,5%



Evolución entre la fase 1 y la fase 2 del estudio completo

- Puertos TCP/IP: Situación muy similar
 - Abrir el puerto TCP/443 y definir la política para el puerto TCP/80
- Visión general de la implementación de HTTPS
 - Incremento en el soporte y priorización de HTTPS: 1-3%
 - Se mantiene el % de downgrades: 2,84%
 - Decremento en los certificados incorrectos: -3%
 - Ligero incremento en el uso de HSTS: 0,5%
- Visión global y detallada (SSL Labs: Grade)
 - Incremento de un 4,5% en los grados: A+, A, y A (desde los grados C-F)
 - Mismos resultados para el grado B

Otros datos curiosos de la fase 2 (SSL Labs)

- HPKP:
 - 2 organizaciones: 5 y 2 hostnames respectivamente
- HPKP-RO: 0
- Protocolos SSL y TLS: (múltiples endpoints)
 - SSL 2.0: 174
 - SSL 3.0: 808
 - TLS 1.0: 2.595
 - TLS 1.1: 2.220
 - TLS 1.2: 2.240
 - TLS 1.3: 4

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

Conclusiones

¡Felicitaciones a todos los organismos participantes!

- Especialmente a los que se han preocupado por mejorar y obtener una calificación de A o A+ (alto o excelente)
 - Esfuerzo, dedicación y constancia
 - Resolución de problemas de integración entre tecnologías y fabricantes
- Continudad así... ¡el objetivo no es acabar aquí!



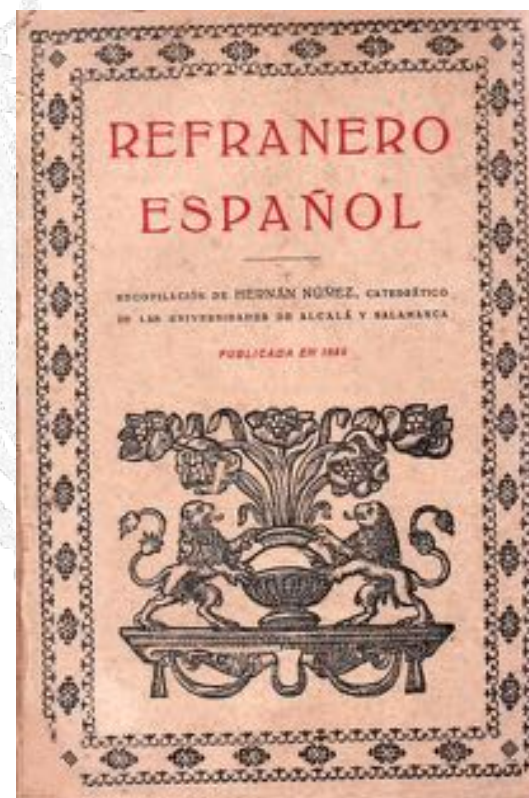
Conclusiones

- Creación de concienciación en la comunidad objetivo: Sector Público
 - Durante el proceso, se han recibido notificaciones de webs claves para el Sector Público dónde no se aplican aún las buenas prácticas de HTTPS
 - "Muchas gracias Miguel M."



El refranero español

“No dejes para
mañana lo que
puedas **HTTP**Sear
hoy...”



¡Muchas gracias!

¿Preguntas?

Raúl Siles

Fundador & Analista de Seguridad

raul@dinosec.com

The logo for Dinosec, featuring a stylized dollar sign symbol followed by the word "Dinosec" in a handwritten-style font.

www.dinosec.com

[@dinosec](#)



➤ 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

