

XIII JORNADAS STIC CCN-CERT



Entorno de Superficie de Exposición



**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCNCERT

Entorno de Superficie de Exposición



Pablo López

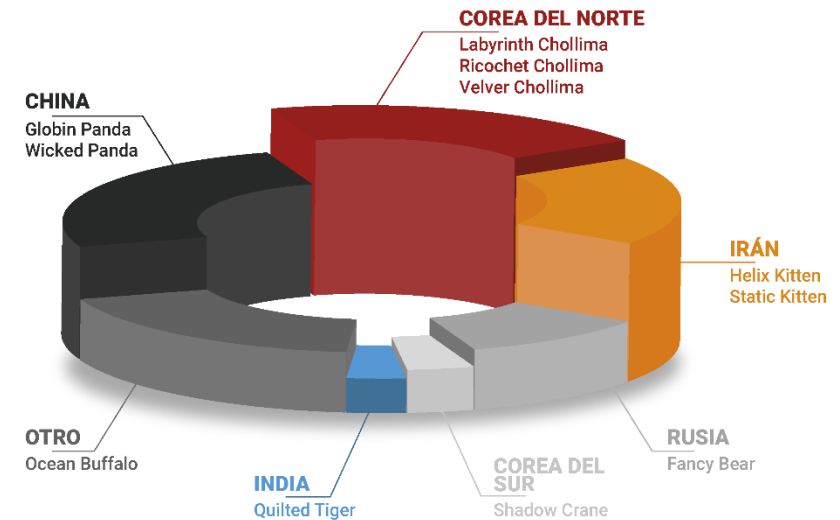
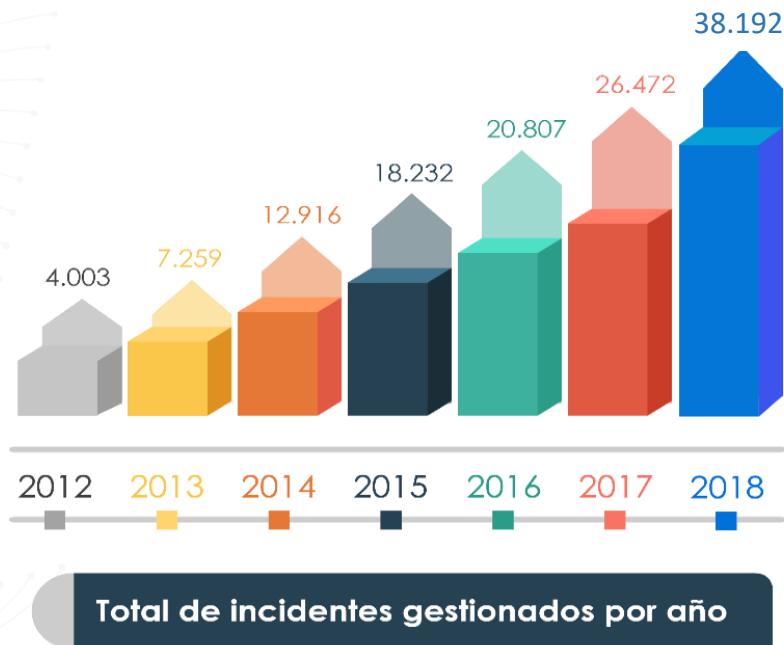
Jefe Área
Normativa y Servicios de
Ciberseguridad

Centro Criptológico Nacional.



La amenaza en el ciberespacio

- ✓ Complejidad y sofisticación de los ataques.
- ✓ Deficiencias en la configuración/bastionado de seguridad.
- ✓ Falta de adopción de buenas prácticas.
- ✓ Carencia de procedimientos de mejora continua.



CIBERAMENAZAS Y ACCIONES QUE USAN EL CIBERESPACIO CON FINES MALICIOSOS

Disrupciones o manipulaciones maliciosas que afectan a elementos tecnológicos.
La acciones que usan el ciberespacio como medio para realizar actividades maliciosas o ilícitas.



CIBERESPIONAJE

Amenazas Persistentes Avanzadas



AMENAZAS HÍBRIDAS

Acciones militares
Ciberataques
Manipulación de la información



CIBERCRIMEN

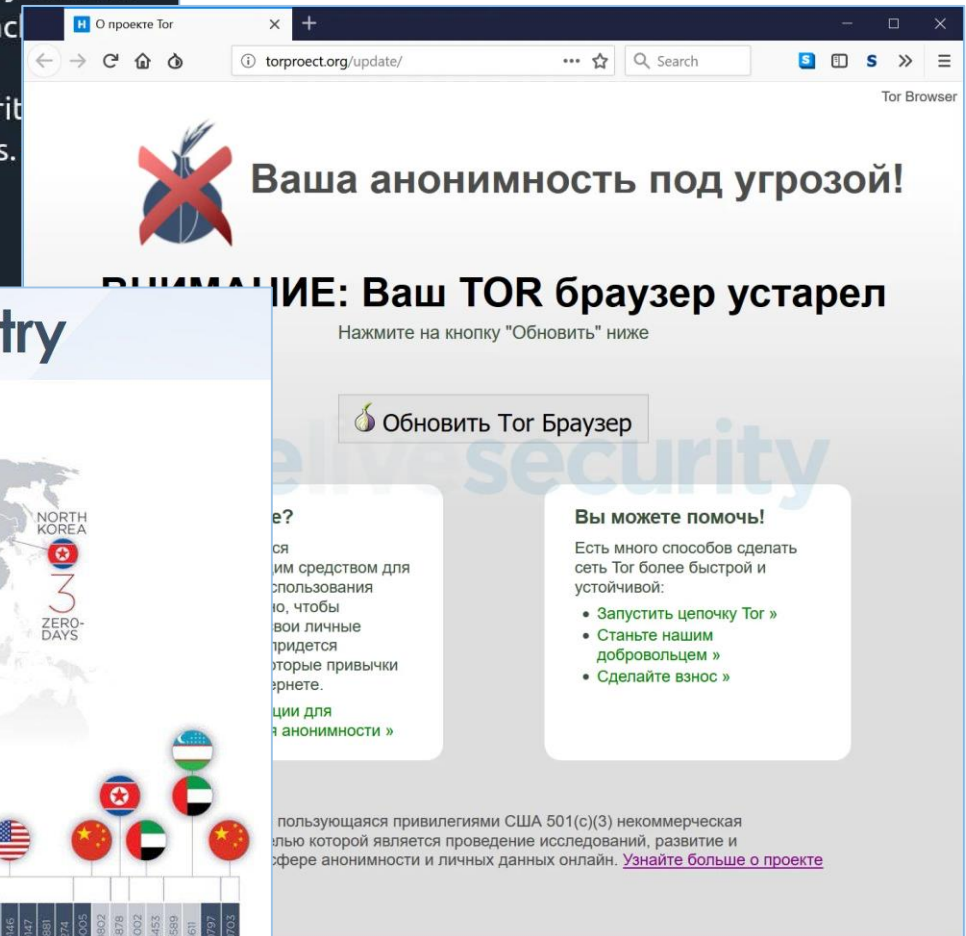
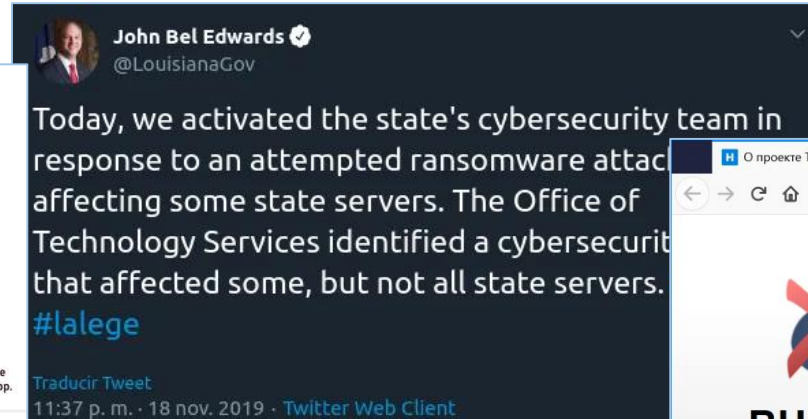
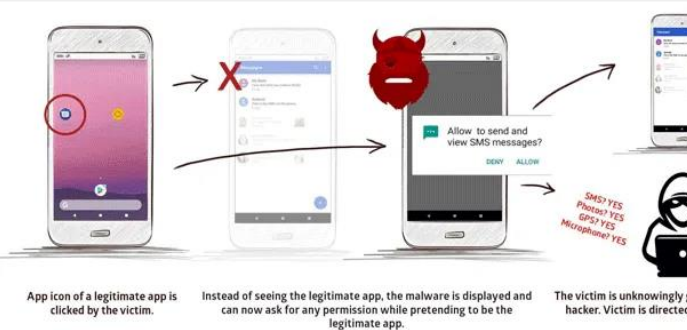
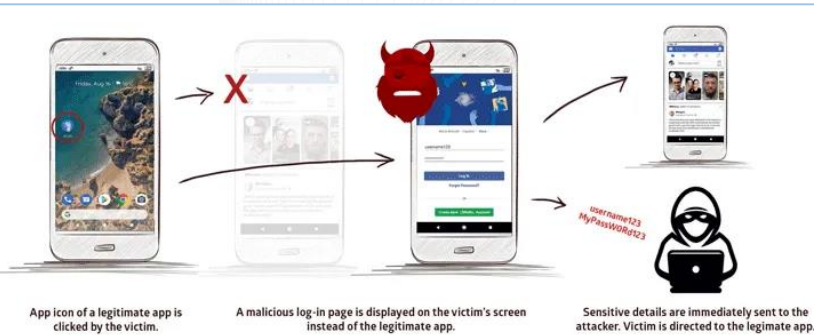
Ciberterrorismo
Ciberdelito



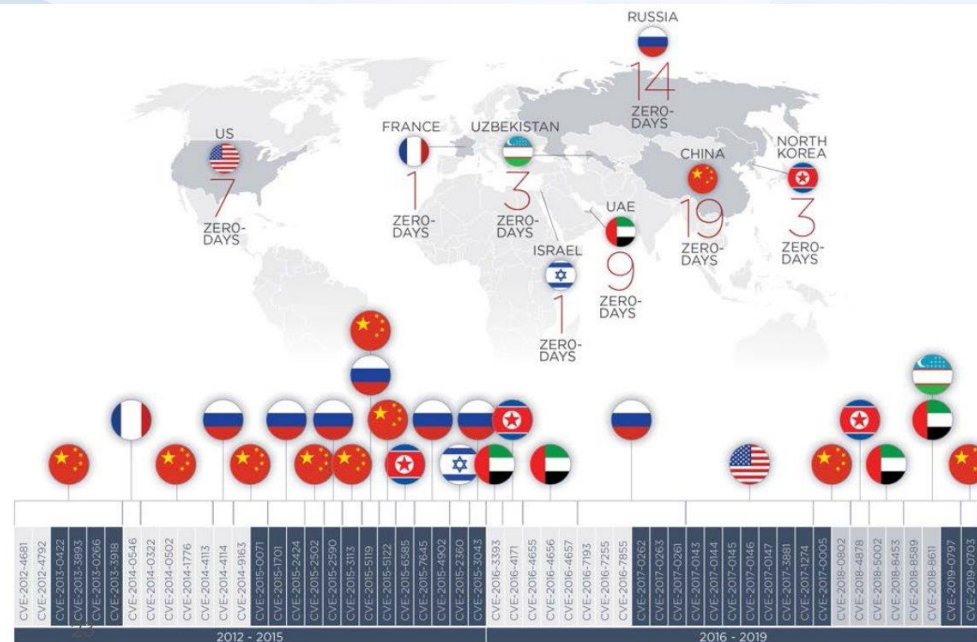
HACKTIVISMO

Ciberataques

Situación de Seguridad – La realidad es muy tozuda...



Zero-Day Usage by Country



WhatsApp Flaw Let Remote Hackers Steal Files and Messages with GIFs

Situación de Seguridad – La realidad es muy tozuda...

Prevención frente

Detalles

Publicado: 08 Octubre 2019

- Informe de Amenazas
- EMOTET

- El CCN-CERT publica un informe de amenazas en la parte pública del portal.
- El objetivo del informe IA-51/19 es divulgar las medidas necesarias para prevenir la campaña de acción por correo electrónico que está afectando de forma significativa a los sistemas de la información.
- Entre los principales puntos que se incluyen se encuentra el vector de ataque, las consecuencias, los mecanismos de propagación y los documentos de seguridad CCN-STIC para el ENS en su categoría alta, dispersión y movimientos laterales, así como las medidas de protección.

El CERT del Centro Criptológico Nacional (CCN-CERT) ha publicado un nuevo Informe de Amenazas en la parte pública como principal misión la prevención de la campaña de código dañino EMOTET con medidas técnicas de las guías CCN-STIC de ENS nivel ALTO.

El punto de entrada o infección del código malicioso EMOTET se produce mediante la ejecución de código embebido en aplicaciones tales como MS Word. Algunas de las consecuencias, una vez que la acción maliciosa se ha producido, son el robo de información, el cifrado del contenido, el robo y exfiltración de contenido sensible o formar parte de una red de tipo "botnet".

Como prevención, el CCN-CERT recomienda que se tomen en consideración todas aquellas medidas que, siendo de aplicación general, quedan recogidas en las guías técnicas de seguridad CCN-STIC que mejoran la seguridad y podrían prevenir su actuación. Entre ellas, tener en cuenta están recogidas en las guías CCN-STIC-599A18 y CCN-STIC-585.

Adicionalmente, no deben desdarse otras potenciales medidas que ofrecerían la protección adecuada, como:

- Aplicar mecanismos integrales de protección Endpoint con análisis y protección frente a comportamientos dañinos, adicional a la detección basada en firmas.
- Aplicar mecanismos de protección en el perímetro, con prevención frente a conexiones internas a sitios de contenido malicioso o de mando y control.

CCN-CERT (08/10/2019)

Informe CCN-CERT IA-51/19 Prevención de la campaña de código dañino EMOTET con medidas técnicas de las guías CCN-STIC de ENS nivel ALTO

Actualizado el informe del CCN-CERT sobre la campaña del troyano EMOTET

Detalles

Publicado: 21 Octubre 2019

- Informe de Amenazas
- EMOTET

- El informe CCN-CERT IA-52/19 Implementación Segura de Microsoft Windows/Office frente a la Campaña EMOTET está disponible en la parte pública del portal.

USO OFICIAL

CCN-CERT IA 51/19

Prevención de la campaña de código dañino EMOTET con medidas técnicas de las guías CCN-STIC de ENS nivel ALTO



Dentro de la guía CCN-STIC de sistema operativo se incluye configuraciones para adecuar los puestos de trabajo o servidores a las diferentes ramas de actualización del sistema operativo según las necesidades de cada organización.

5. CONCLUSIONES

Tomando en consideración las medidas aplicables que recogen las guías de seguridad CCN-STIC para la categoría alta, se puede determinar que las acciones dañinas consecuencia de códigos como EMOTET pueden ser controladas, bien impidiendo su acción o bien limitando la misma. Solo acciones conscientes del usuario y degradando la seguridad existente podrían suponer un riesgo general para la organización, habiendo aplicado las medidas de protección adecuadas.

Además, debe tomarse en consideración que en general la aplicación efectiva de los principios de mínima exposición, mínimo privilegio y seguridad continua, sumada a la concienciación en materia de ciberseguridad, que quedan fielmente recogidas y son de inspiración en el Esquema Nacional de Seguridad, serían consideraciones a tomar siempre en cuenta para limitar o impedir acciones dañinas a través de campañas tales como la originada por el código EMOTET.

implementación segura en un entorno definido, se puede determinar que las acciones dañinas consecuencia de códigos como EMOTET pueden ser controladas, bien impidiendo su acción o bien limitando la misma.

Se trata del informe de la última actualización de su portal. Se trata del informe de la última actualización de su portal.

Segura en un entorno definido

sistemas Windows y proporciona

embebido desde un documento de Word, son el proceso de secuestro de información.

nivel ALTO

Necesidad de implementar ciberseguridad



Prevención



Detección



Respuesta

¡¡Ciberseguridad es generar Confianza!!

La adaptación a las nuevas amenazas implica **MEJORAR LAS CAPACIDADES DE VIGILANCIA**
y diseñar respuestas cada vez más eficaces frente a los ataques



**Determinación de la
Superficie de Exposición**



**Mejora
Continua**



**Reducción del Tiempo de
Respuesta**

SOC

Security audits or
assessments
against standards

Alerts and warnings
Incident handling
Vulnerability handling
Artefact handling
Forensics handling
Technology watch

Configuration & maintenance of
tools, apps and infrastructure

Intrusion detection

Risk analysis

Business continuity and
Disaster Recovery

Planning

Security consulting

Education and security
awareness training

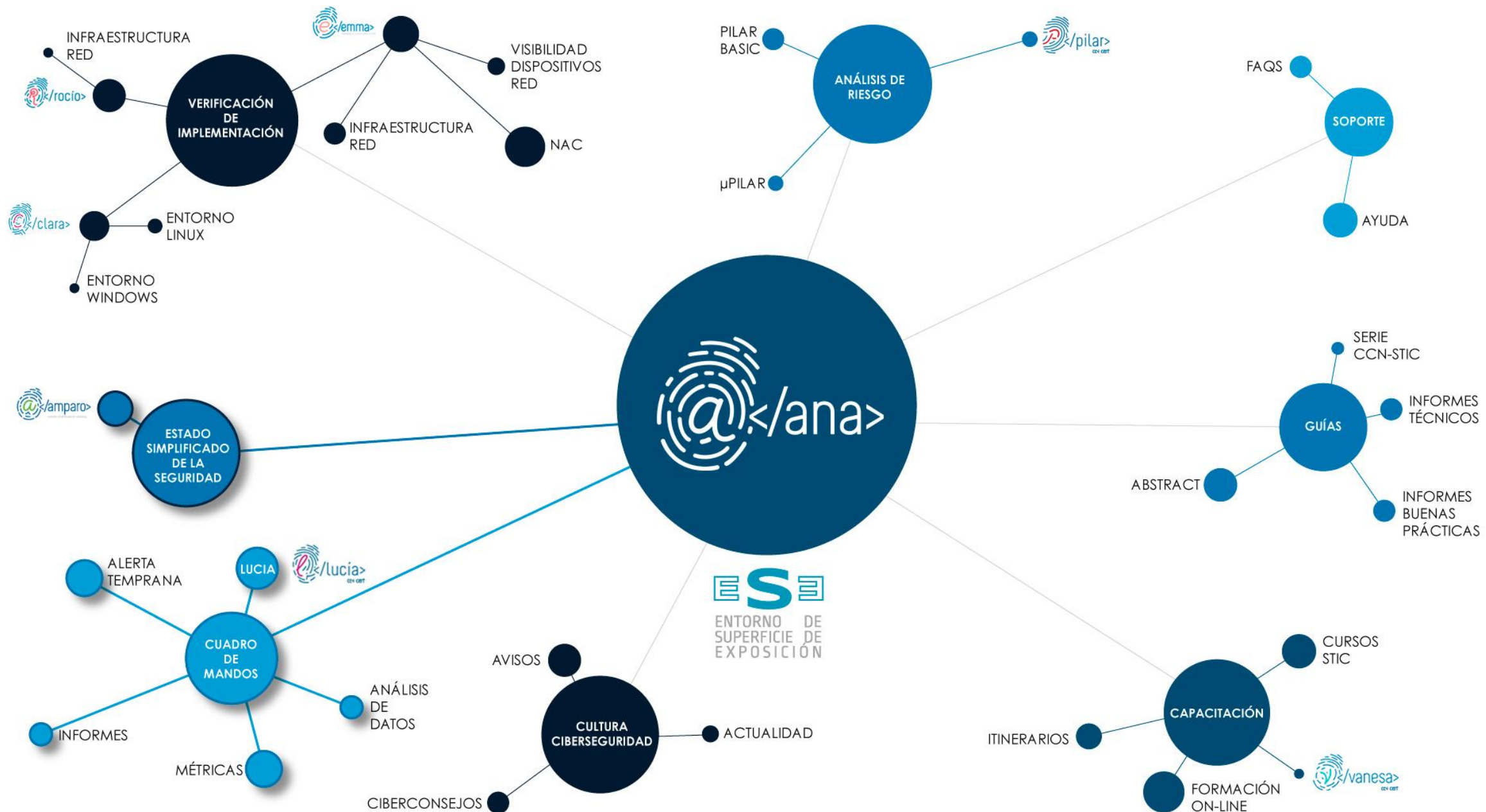
CSIRT

Real-time monitoring
Reporting
Network mapping
Vulnerability scanning
Penetration testing
Insider threat
investigation



La importancia de Medir la Seguridad







La Importancia de Educar

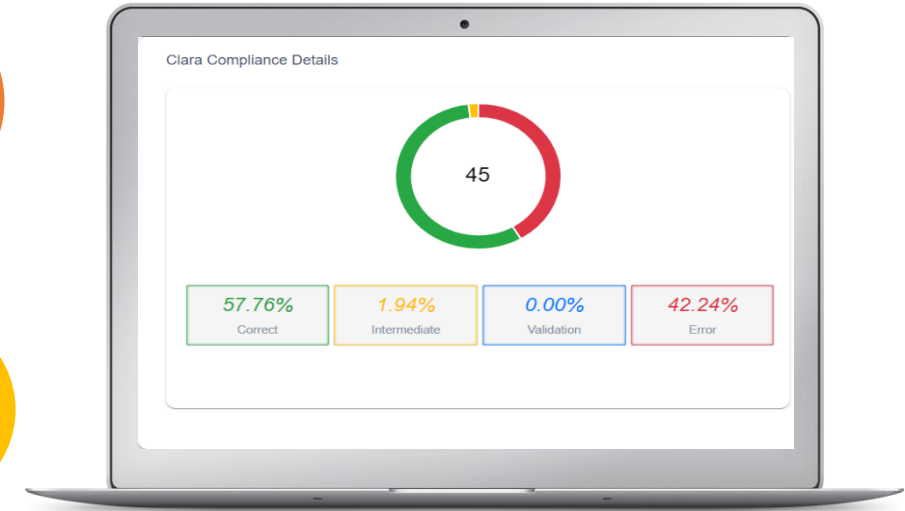


21
cursos a distancia

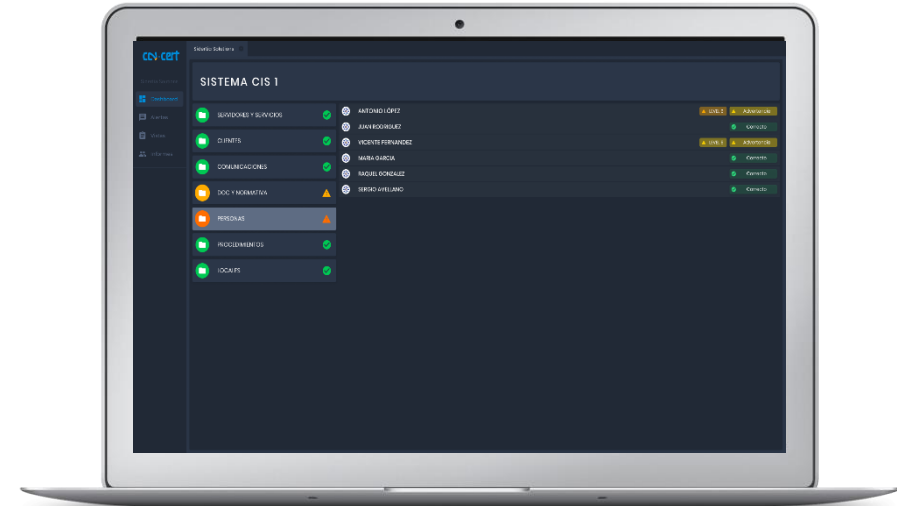




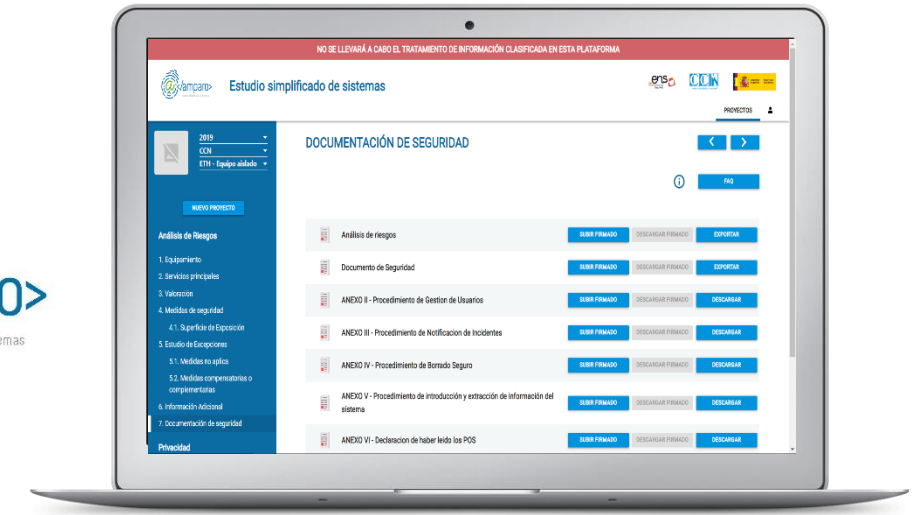
- Acceder en tiempo real a problemas localizados, reproducirlos y seguir su **evolución en el tiempo**.
- **Generar dinámicamente informes del estado** real de la entidad por departamento, servidor, aplicación o cualquier activo definido.
- Organizar la información proporcionando **múltiples** vistas/cuadro de mandos a los usuarios.
- **Centralizar y normalizar** todas las inspecciones de seguridad realizadas.
- **Alerta temprana** mediante interacción directa y detallada de las incidencias encontradas permitiendo una **notificación oportuna** sin dilación indebida.



- **Identificación de software (CPE)** básico a partir integración con CLARA.
- **Informe ejecutivo/técnico** de CLARA.
- **Conformidad o no conformidad** de los activos.
- **Evolución del grado de no cumplimiento** de los activos.
- **Cuadro de mando/presentación** según jerarquía diseñada en CLARA.
- **Concordancia CVE/CPE** de forma automática **CLARA/Nessus** y **manual**.
- **Alerta de vulnerabilidades** potenciales asociadas al software presente en los activos (CPE).



- Se **estructuran y representan** sistemas, servicios y activos.
- **Gestión de activos**, alertas sobre el estado de seguridad (foto dinámica).
- Múltiples tipos de activos: **tecnológicos y no tecnológicos**.
- Los activos presentan una criticidad en base a su relación con el sistema.
- El análisis permite **predecir** las incidencias de seguridad.
- Se **analiza y se profundiza** en brechas de seguridad.
- **Integración** y hallazgos desde **distintas soluciones CCN-CERT**.
- Se **comprueba** el origen del **riesgo** y se determina la posible **mitigación**.
- El “entorno” **notifica una alerta**.



- **Estudio simplificado de sistemas** para facilitar y agilizar el proceso de cumplimiento de sistemas.
- Simplicidad al permitir la **generación**, de **manera guiada**, de la documentación de seguridad necesaria.
- **Modelos predefinidos** de riesgos, documentación de seguridad y procedimientos que se adaptan a los distintos escenarios existentes.
- Agilidad, al **reducir la curva de aprendizaje** del usuario responsable del sistema.
- Obtención de **resultados de manera casi inmediata**.
- Control al establecer un **marco centralizado** de los principales aspectos de un sistema que maneja información sensible.





- **Implementar seguridad** y no limitarse a realizar análisis de riesgos y documentar procedimientos.
- **Anticiparse** y buscar **soluciones**.
- Mejora basada en cumplimiento de **requisitos consensuados**.
- Analizar **medidas compensatorias**.
- Lograr **estándares de seguridad acreditables** de acuerdo a las inspecciones STIC llevadas a cabo.
- La mejora continua implica **complementar la implementación** de medidas de seguridad con un **incremento de la vigilancia**.
- **Sistema compensatorio de vigilancia**.



[CL/01] Ecosistema de la ciberseguridad

El **ECOSISTEMA DE LA CIBERSEGURIDAD** se enfrenta a un **INCREMENTO** constante en el número, sofisticación y complejidad de los ciberataques.



[CL/02] Implementar seguridad

No se puede dejar de hacer uso de la tecnología, pero se debe **IMPLEMENTAR SEGURIDAD**, utilizar **TECNOLOGÍA CERTIFICADA** y abusar del **SENTIDO COMÚN**.



[CL/03] Superficie de exposición

La **SUPERFICIE DE EXPOSICIÓN** es susceptible de **INCREMENTAR**: redes sociales, teléfonos móviles, BYOD, IoT... y hay que manejarla evitando ser un objetivo fácil de atacar (No ser un Objetivo Blando).



[CL/04] Tiempos de respuesta

La ciberseguridad pasa por **MEDIR**, conocer la superficie de exposición y reducir al mínimo los **TIEMPOS DE RESPUESTA**.



[CL/05] Mejora continua

Adoptar la **MEJORA CONTINUA** como reto a lograr, foto dinámica a optimizar progresivamente **EN BASE A COMPROMISOS E HITOS** adoptados por todos los actores involucrados.



[CL/06] Buenas Prácticas

Educar al usuario de la tecnología en procedimientos y **BUENAS PRÁCTICAS** reduce la superficie de exposición,

COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional