cesicat

Equipo de Respuesta a Incidentes

VIII OWASP Spanish Chapter Meeting

¿Qué es un incidente de seguridad?

¿Qué es un incidente de seguridad?

CERT/CC define un incidente de seguridad como:

"Cualquier evento adverso, real o potencial, ***vinculado a la seguridad de los sistemas*** *de información y sus redes. Así como el acto de* ***violar una política de seguridad*** *de forma implícita o explicita".*

cesicat

¿Qué es un incidente de seguridad?

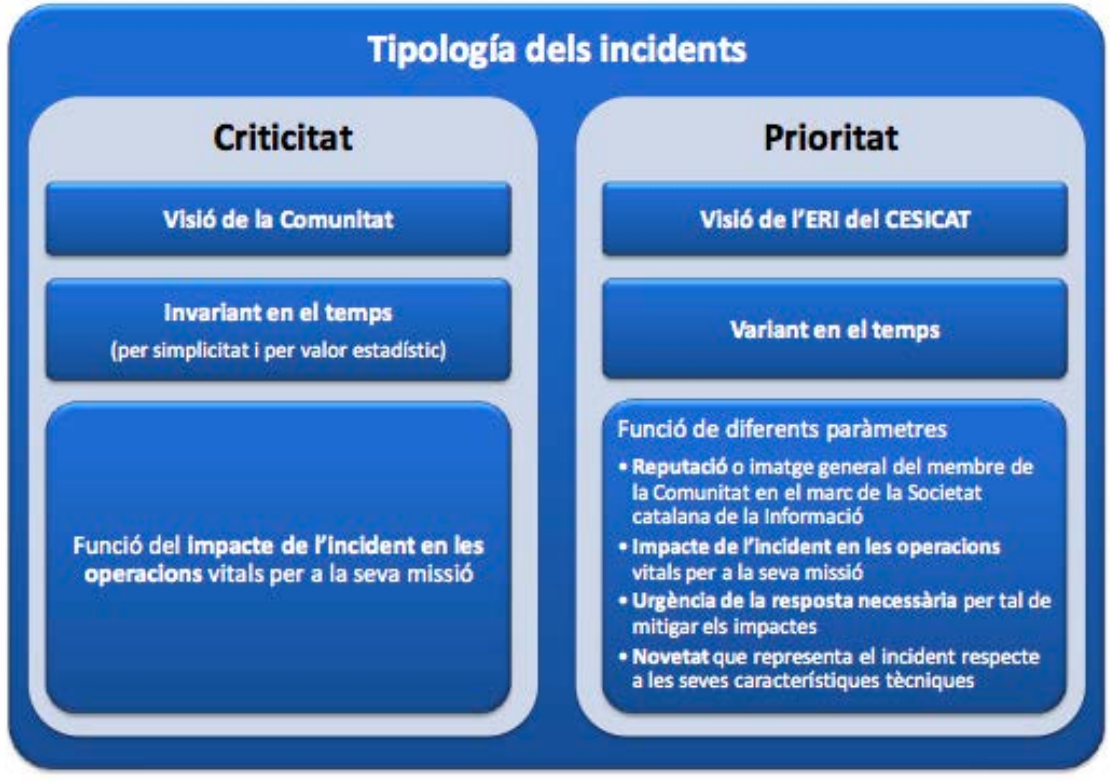
Actualmente clasificamos de **37 formas** diferentes los incidentes.

Categoria d'incidents	Tipus d'Incident
Contingut Abusiu	Spam
	Assetjament
	Contingut no autoritzat per la política
Codi Maliciós	Virus
	Cuc
	Troià
	Spyware
	Dialer maliciós
Recollida d'informació	Escaneig
	Escaneig aplicació Web
	Sniffing
	Enginyeria Social
Intents d'Intrusió	Explotació de vulnerabilitats conegudes
	Cross-Site Scripting
	Injecció SQL
	Injeccions de Fitxers Remota
	Injecció d'altres tipus
	Intents de Login
	Atac desconegut
Intrusions	Compromís compte privilegiat
	Compromís compte no privilegiat
	Compromís d'aplicació
Atac a la Disponibilitat	DoS
	DDoS
	Sabotatge
	Fallada (programari / maquinari)
	Error humà
Atac a la Confidencialitat i Integritat de la informació	Accés no autoritzat a la informació
	Modificació no autoritzada de la informació
Frau	Ús no autoritzat de recursos
	Copyright
	Suplantació
	Phishing
Investigació digital	Comunicacions mòbils
	Investigació a Internet
	Suport accions policials
Altres	Altres

cesicat

¿Qué es un incidente de seguridad?

Un incidente de seguridad, se gestiona en función de su tipología.



– La prioridad determina la dedicación de recursos y el tiempo máximo para la resolución del incidente de seguridad.
– La clasificación del incidente y su prioridad también determinan el coste €€€.

cesicat

¿Qué es un Equipo de Respuesta a Incidentes?

¿Qué es un Equipo de Respuesta a Incidentes?

Un Equipo de Respuesta a Incidentes (ERI) provee servicios y da soporte para prevenir, gestionar y responder ante los incidentes de seguridad de la información.

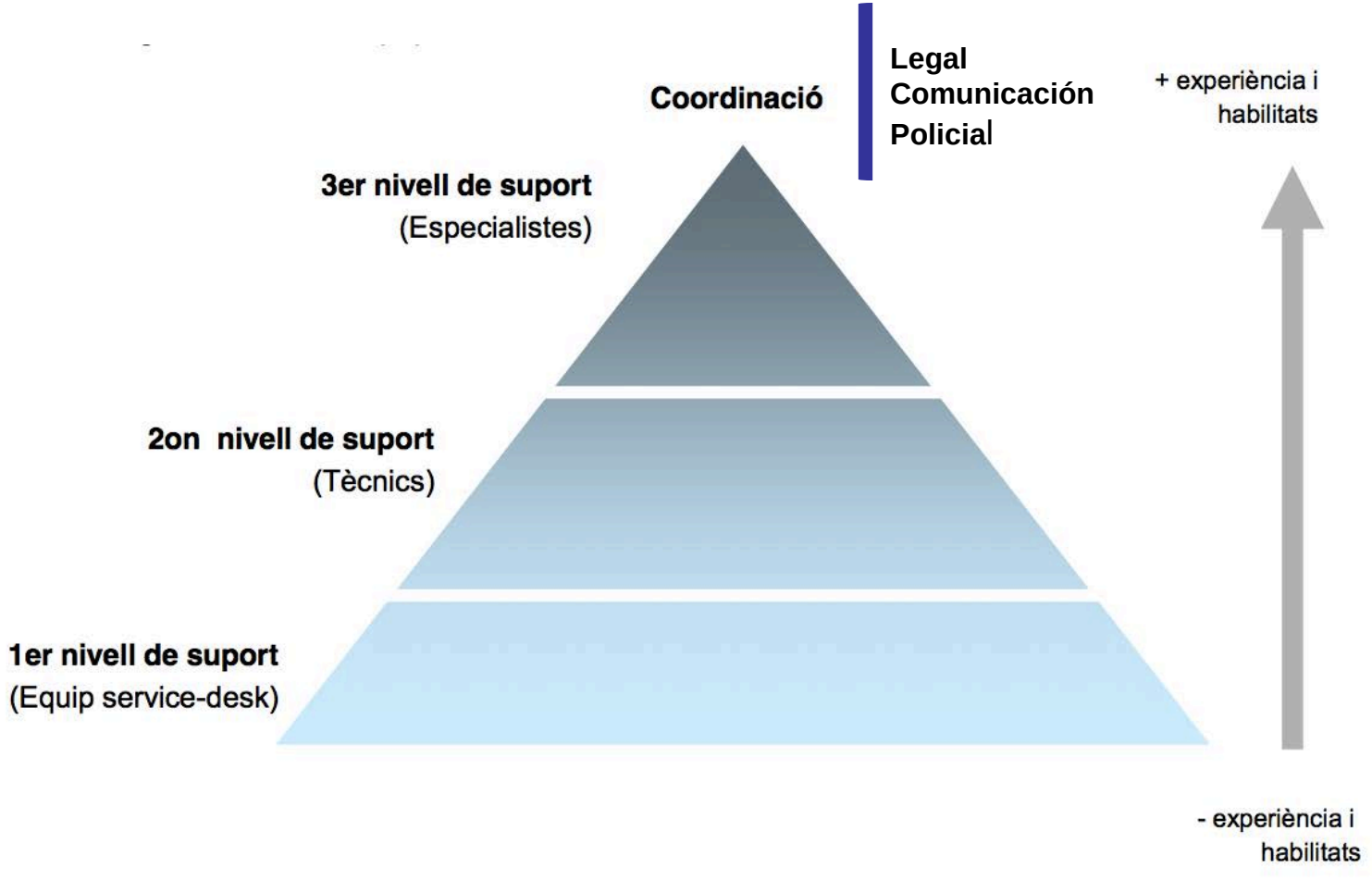
El Equipo de Respuesta a Incidentes de CESICAT da soporte a:

- Gobierno de Catalunya y administraciones locales
- Fuerzas policiales
- Ciudadanía
- Empresas
- Universidades y centros de investigación

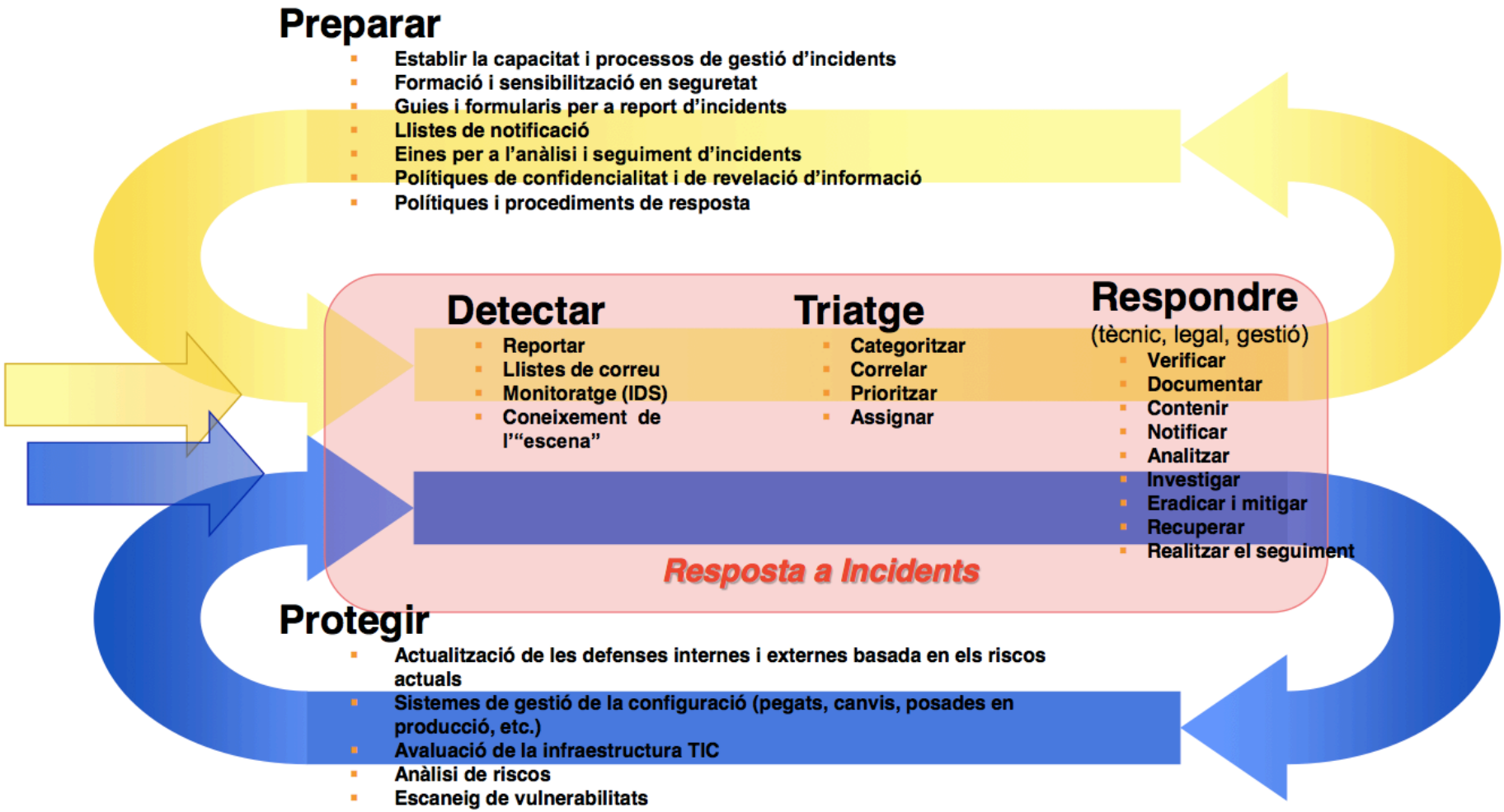
cesicat

Equipo de Respuesta a Incidentes

- Estructura Genérica del Equipo de Respuesta a Incidentes



Proceso del Equipo de Respuesta a Incidentes



cesicat

Modelo documental del Equipo de Respuesta a Incidentes

- **Políticas y normas**
  - Política para el intercambio de información con terceros.
  - Norma de uso de los dispositivos del laboratorio.
  - …
- **Procedimientos**
  - Procedimiento para la adquisición de evidencias
  - Procedimiento para la clasificación de incidentes
  - …

- **Instrucciones operativas**
  - Instrucciones para el clonaje de discos duros
  - Instrucciones para el despliegue de contramedidas contra el SPAM.
  - …

Servicios

- **Respuesta remota a incidentes**
  - Resolución de consultas.
  - Avisos y alertas.
  - Gestión de vulnerabilidades críticas.
  - Coordinación con áreas internas de CESICAT y con terceros.
  - Despliegue de sistemas de detección para ser más proactivos.
  - Análisis y asesoramiento en la aplicación de contramedidas.

- **Soporte in-situ**
  - Asesoramiento y coordinación en la gestión de un incidente.
  - Despliegue de contingencias
  - Adquisición de evidencias

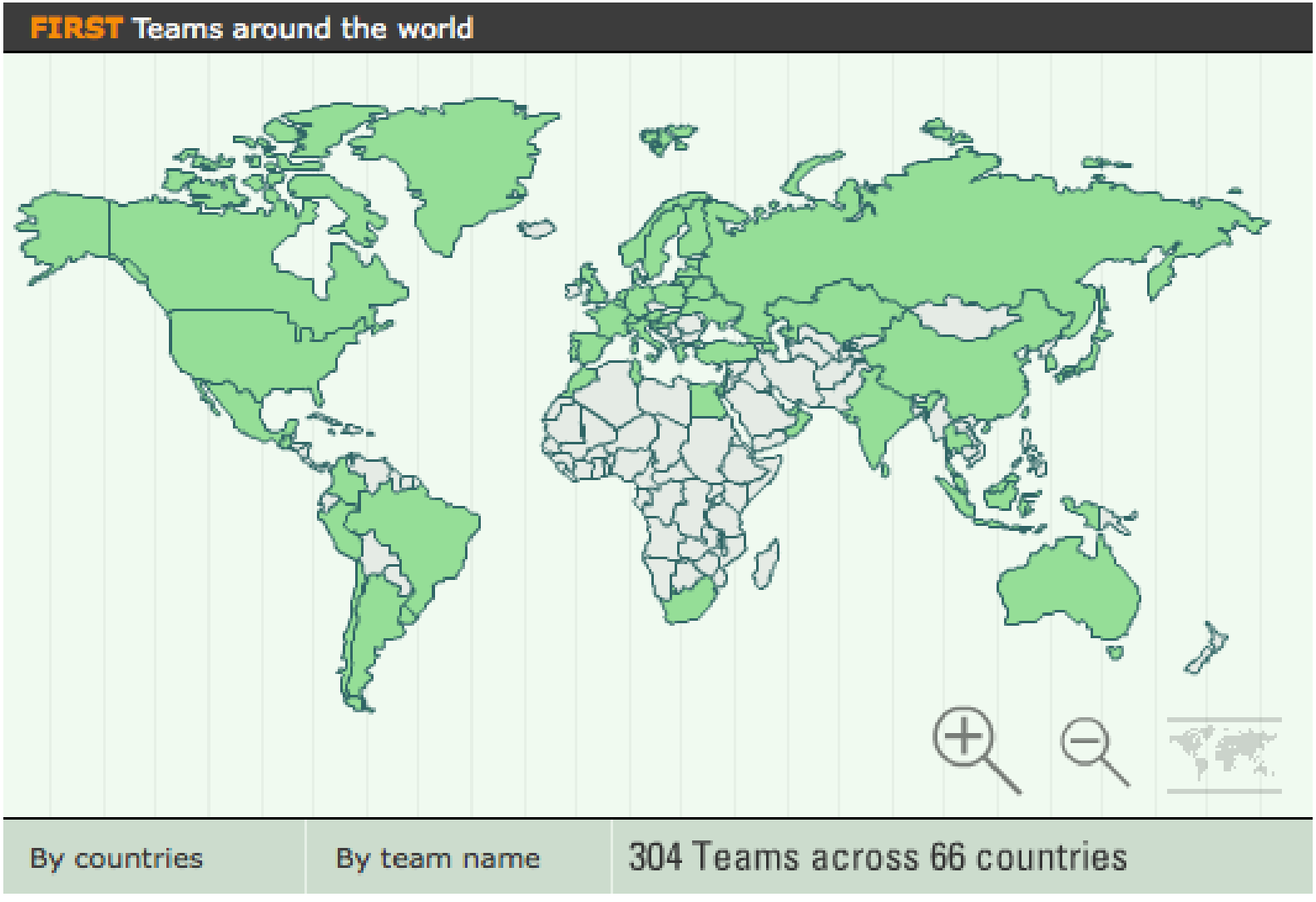
- **Análisis de laboratorio**
  - Análisis de artefactos
  - Investigación de vulnerabilidades y de la seguridad de nuevas tecnologías
  - Estudio de nuevas contramedidas.

cesicat

Red de CERT's

TF-CSIRT
Trusted Introducer

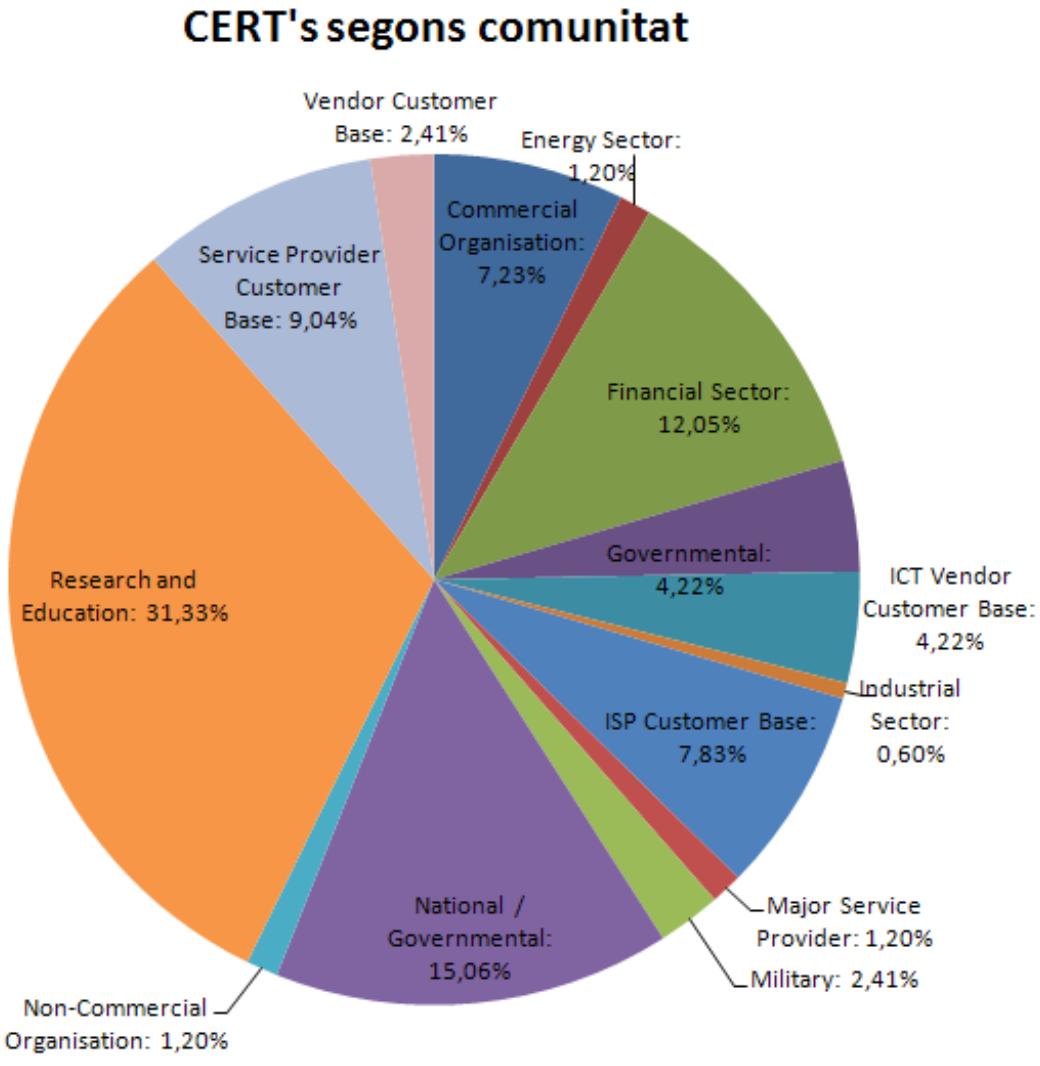
Red de CERT's (304 Equipos)



Red de CERT's (304 Equipos)

cesICAT

Red de CERT's


CERT's segons comunitat
Vendor Customer Base: 2,41%
Energy Sector: 1,20%
Commercial Organisation: 7,23%
Service Provider Customer Base: 9,04%
Financial Sector: 12,05%
Governmental: 4,22%
Research and Education: 31,33%
ICT Vendor Customer Base: 4,22%
Industrial Sector: 0,60%
ISP Customer Base: 7,83%
National / Governmental: 15,06%
Major Service Provider: 1,20%
Military: 2,41%
Non-Commercial Organisation: 1,20%

Red de CERT's

En España existen actualmente 15 CERT's

- 6 son del sector privado (e-LaCaixa, MAPFRE, s21sec, Telefonica, INCITA, CyberSOC CERT).
- 9 son del sector público (CCN, INTECO, CESICAT, esCERT, IRIS-CERT, Andalucía-CERT, CSIRT-CV, COSDEF, CESCA)

La red de CERT's establece la **voluntad**, de las entidades adscritas, de compartir información y de ayudarse mutuamente para la resolución de incidentes.

Colaboración con terceros

El ERI colabora activamente con diferentes entidades:

ETC...

Herramientas de soporte

La gestión del ERI, actualmente se sustenta en dos herramientas:

- Gestión de tickets
- Gestión del Conocimiento

Herramientas de soporte – Gestión de tickets

Herramienta de gestión de tickets

- Es el punto de entrada de información de cualquier incidente.
- Es la herramienta de comunicación con el afectado.
- Permite realizar un tracking de toda la gestión de la comunicación con los clientes y de las acciones que el Equipo realiza por cada incidente.
- Ayuda a entender que incidentes son mas prioritarios que el resto, cuáles deben ser atendidos, quién es la persona encargada de gestionar un incidente concreto, etc.
- La herramienta permite extraer automáticamente métricas e indicadores del servicio.

Herramientas de soporte – Gestión del conocimiento

Herramienta de gestión del conocimiento

- La herramienta es un sistema Wiki, que actúa como repositorio central de documentación del ERI.
- Encontramos todas las políticas, normas, procesos, instrucciones y documentación relativa a investigaciones.
- Al ser una Wiki, permite:
  - Inter-relación de la información.
  - Encontrar la información ágilmente (buscador, clasificación por categorías, tags, etc.).
  - Colaboración en la creación y edición del contenido
  - Comentarios y puntuación del contenido (I like it!)
  - Restricción de acceso al contenido

Laboratorio

CESICAT dispone de un laboratorio para investigar incidentes.

Infraestructura del laboratorio

- Red aislada
- Servidor ESXi per a la virtualización de sistemas.
- Caja fuerte y caja ignifuga.
- 2 Workstation de trabajo (con diferentes herramientas instaladas + bloqueador de escritura).
- 2 Maletines forense.
  - Clonadora de discos
  - Bloqueadores de escritura
  - Disco duro para la adquisición de evidencias
  - Lector de tarjetas
  - Cámara de fotos
  - Cables y adaptadores
  - Etiquetadora
  - Formularios de adquisición
- 1 Maletín TELCO (tarjeta wifi, antenas, funcube, pinapple, etc…)
- Bolsas de Faraday

Laboratorio (II)

Software del Laboratorio

Maquinas Virtuales de prueba (testbeds) :

- Windows XP (SP1, SP2, SP3), Windows 7, Windows 2003, Windows 2008, Solaris, Linux, etc

Maquinas Virtuales con herramientas para:

- Búsqueda de información: Maltego
- Investigación de logs: Splunk, grep, sed, cut y awk... xD
- Análisis de intrusiones: Backtrack, Nessus, Accunteix, w3af
- Análisis de tráfico de red: Wireshark, NetworkMiner
- Análisis y captura de datos: Encase, Helix 3 pro, F-Response, VM Insectra, Paraben
- Análisis de comportamiento: Sysinternals, Norman Analyzer, FTK Analyzer
- Ingeniería inversa: HexRays IdaPro
- Ataques contra el cifrado: JTR, Hashcat, Rainbow tables, etc.

- Scripts propios en Python y **Ruby**.

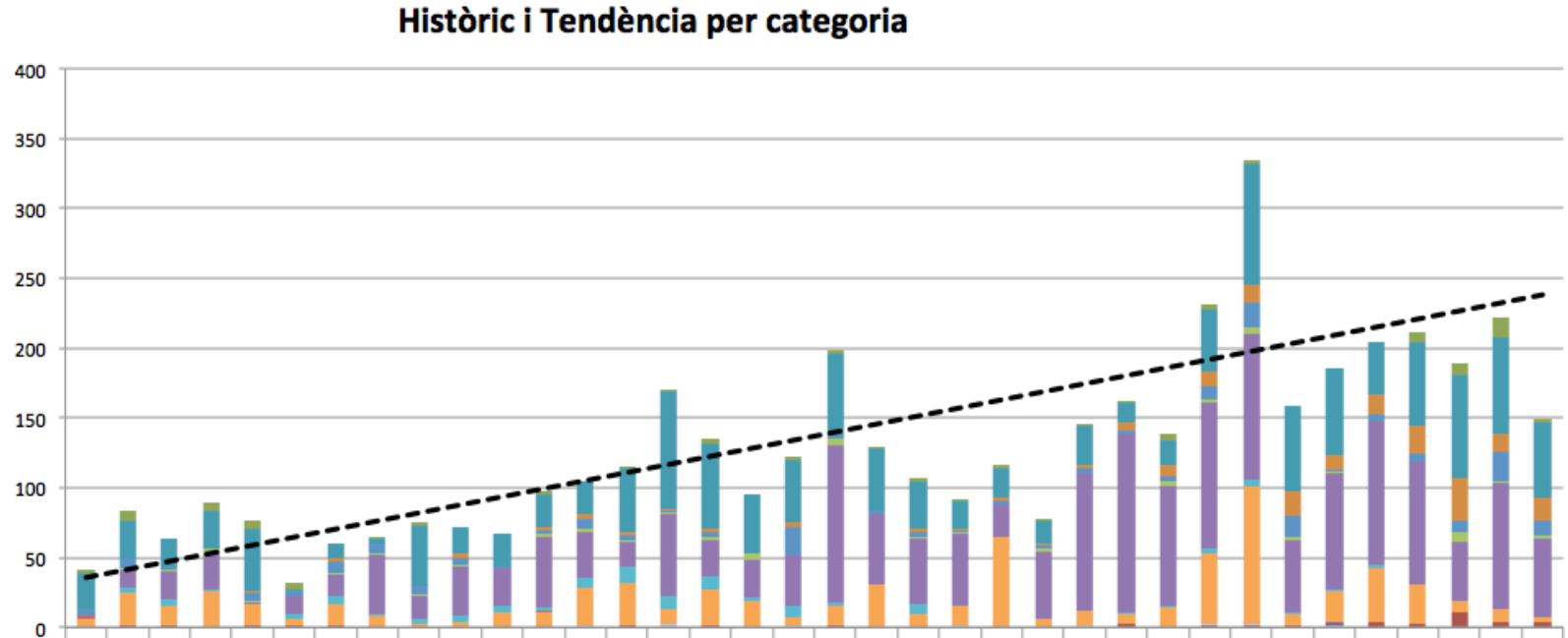
Casos de éxito

Casos de éxito del equipo de respuesta a incidentes:

- Gestión de un total de 4.926 incidentes
  - 2011 ➔ 820 incidentes
  - 2012 ➔ 1.470 incidentes
  - 2013 ➔ 2.636 incidentes

- Cooperación en la desarticulación internacional de la Botnet Bamital con Symantec, Mossos d'Esquadra, Guardia Civil y Microsoft.

Incidentes gestionados por categoría



	2011/01	2011/02	2011/03	2011/04	2011/05	2011/06	2011/07	2011/08	2011/09	2011/10	2011/11	2011/12	2012/01	2012/02	2012/03	2012/04	2012/05	2012/06	2012/07	2012/08	2012/09	2012/10	2012/11	2012/12	2013/01	2013/02	2013/03	2013/04	2013/05	2013/06	2013/07	2013/08	2013/09	2013/10	2013/11	2013/12
Atac a la Disponibilitat	2	7	0	5	6	5	0	1	2	0	0	2	0	1	1	3	0	2	2	1	2	1	2	1	2	1	5	3	2	0	0	0	7	8	14	2
Codi Maliciós	26	26	21	27	45	1	11	3	43	19	23	23	24	46	84	62	42	45	59	45	34	20	21	17	28	14	18	45	87	60	62	37	59	74	69	54
Contingut Abusiu	0	0	0	0	1	0	2	0	1	3	0	3	3	2	1	2	0	3	0	0	3	1	3	1	2	6	8	11	13	18	10	14	20	31	13	17
Frau	4	8	1	1	6	4	8	7	5	5	2	2	8	4	2	3	0	20	2	2	3	1	2	3	3	3	4	9	17	15	1	5	6	8	21	10
Intent Intrusió	0	1	1	3	1	0	1	1	1	1	0	2	2	1	1	3	5	0	5	0	1	1	0	2	0	0	3	2	5	3	1	0	0	7	2	3
Intrusió	0	13	20	26	1	12	15	42	17	36	26	51	33	17	58	25	27	36	112	50	47	52	23	48	99	127	86	104	104	51	84	103	88	42	90	56
Investigació digital	1	3	4	1	0	4	6	1	3	4	5	2	7	12	10	10	2	9	3	0	7	0	0	0	0	1	1	4	5	1	1	2	0	0	0	0
Signatures IDS personalitzades	2	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Gestió/Resolució de vulnerabilitats	6	24	15	26	16	5	16	9	3	4	11	11	27	31	11	26	19	6	14	31	10	14	65	6	11	8	14	51	98	9	22	39	29	8	9	3
Alerta Amenaces	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	3	0	0	0	0	0
Recollida Informació	0	0	0	0	0	0	0	0	0	0	0	0	1	0	2	0	0	1	0	0	0	1	0	0	1	0	0	1	1	0	1	0	0	0	0	0
Altres	0	1	1	0	1	1	1	0	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	2	0	1	1	1	0	4	2	11	4	4
Total - Casos nous	41	83	63	89	77	32	60	64	75	72	67	97	105	116	171	139	97	123	198	129	107	91	116	78	148	164	143	257	363	181	209	230	231	245	249	216

cesicat

¿Cómo reportar un incidente?

Para reportar un incidente CESICAT pone a disposición dos canales de comunicación:

Tel: +34 902 112 444

e-mail: cert@cesicat.cat

“No se trata de ser mejor que otro, se trata de ser mejor de lo que eras tu mismo el día anterior”

- Ferrán Adrià

¿Alguna pregunta?

www.cesicat.cat