Qué es **INCIBE**

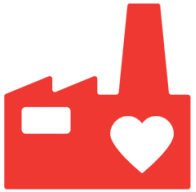
GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Qué es **INCIBE**

Entidad de referencia para el **desarrollo de la ciberseguridad y de la confianza digital** de:

Ciudadanos

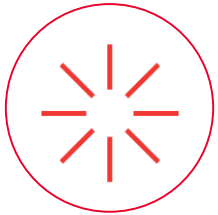


Empresas, en especial de **sectores estratégicos**

Sociedad Estatal dependiente de la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital que lidera diferentes **actuaciones para la ciberseguridad a nivel nacional e internacional**

Nuestra historia

2006



Nace INTECO

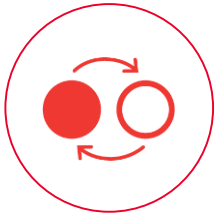
Instituto Nacional de Tecnologías de la Comunicación

2012

INTECO

Se focaliza en el mundo de la ciberseguridad

2014



Se transforma en INCIBE

Instituto Nacional de Ciberseguridad de España

Qué hacemos

Apoyo al desarrollo de la industria, I+D+i y talento

Servicios de Ciberseguridad

Tecnologías de ciberseguridad

Servicios de ciberseguridad: CERTSI

Año 2012 → Acuerdo Marco de Colaboración:

Secretaría de Estado de Seguridad	+	Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información	=	certsi_ CERT DE SEGURIDAD E INDUSTRIA
CNPIC		**INCIBE**		**CERTSI**
				Apoyo tecnológico FCSE

CERT de Seguridad e Industria (CERTSI)

certsi_
CERT DE SEGURIDAD E INDUSTRIA

Referencia para la **resolución técnica de incidentes de ciberseguridad** que afectan a ciudadanos y empresas

Prevención

Detección

Análisis

Respuesta

Notificación

ciudadanos

empresas

operadores críticos

Servicios

Detección, Análisis,
Respuesta y Notificación

Intercambio
de información

Ciberejercicios

Capacitación

Relaciones y alianzas

Servicio antibotnet con ISPs y operadores

Convenio entre SES y SETSI para la protección de infraestructuras críticas nacionales y lucha contra el ciberdelito

NDAs con empresas y operadores estratégicos

A nivel internacional: foros especializados e implicación en iniciativas comunitarias

Organización de los Estados Americanos

enisa European Network and Information Security Agency

FIRST Improving Security Together

APWG

European Commission

Incidentes por público objetivo

Incidentes gestionados
en 2016

115.257

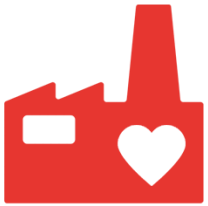
110.293

Ciudadanos
y empresas

Red IRIS

4.485

Red Académica
(RedIRIS)



479

Operadores
críticos

Tipos de incidentes 2016

76.811	Virus, troyanos, gusanos, spyware
14.373	Acceso no autorizado
11.843	Fraude
10.279	SPAM
1.038	Otros
495	Denegación de servicio
381	Escaneos de red
37	Robo de información

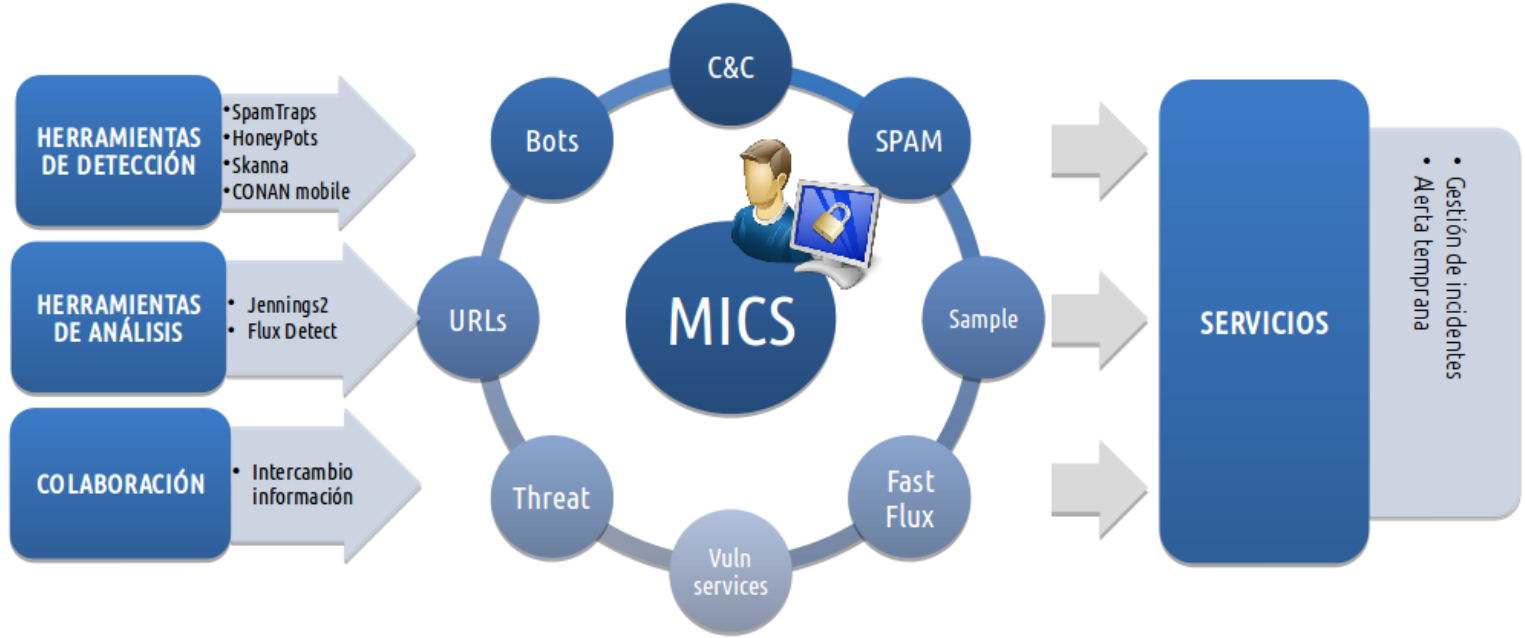
Respuesta incidentes	Detección proactiva	Alerta temprana	Detector incidentes	Informatio n gathering	Ciberejerci cios	Compartic. amenazas	Servicio Preventivo

Análisis y resolución de incidentes en Operadores

Servicio en formato 24x7x365

Servicios del CERT

Respuesta incidentes	Detección proactiva	Alerta temprana	Detector incidentes	Informatio n gathering	Ciberejerci cios	Compartic. amenazas	Servicio Preventivo



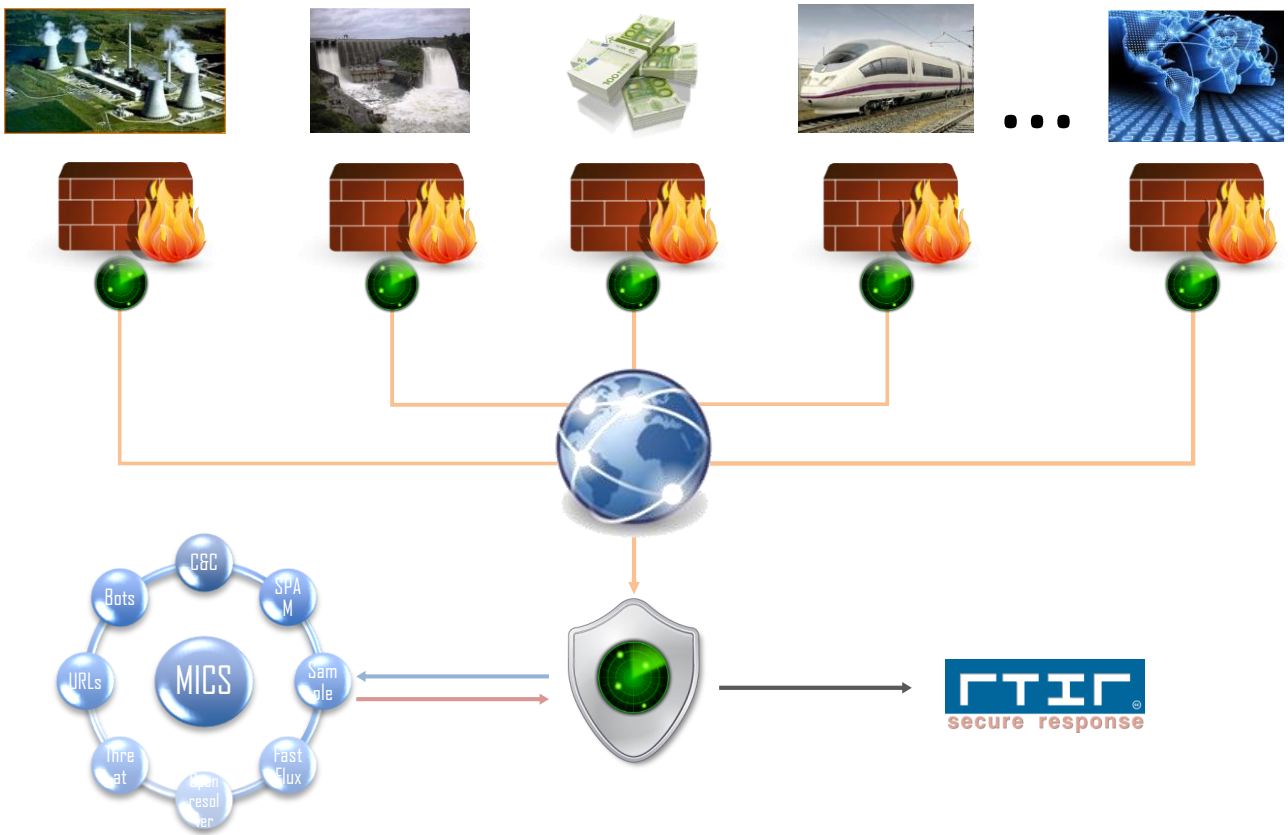
Detección | Análisis | Valor

Vulnerabilidades 0day

- Criticidad
- Recursos afectados
- Descripción
- Solución / mitigación

Servicios del CERT

Respuesta incidentes	Detección proactiva	Alerta temprana	**Detector incidentes**	Information gathering	Ciberejercicios	Compartic. amenazas	Servicio Preventivo



Servicios del CERT

Respuesta incidentes	Detección proactiva	Alerta temprana	Detector incidentes	Information gathering	Ciberejercicios	Compartic. amenazas	Servicio Preventivo

Objetivo: informe personalizado de la visión de un posible atacante.

- Posibles vulnerabilidades detectadas
- Posible software vulnerable
- Dominios registrados
- Subdominios encontrados
- IPs activas
- Servidores web encontrados
- Vigencia de certificados
- Protección ante suplantación

Información exclusivamente a partir de fuentes públicas.

Servicios del CERT

Respuesta incidentes	Detección proactiva	Alerta temprana	Detector incidentes	Informatio n gathering	Ciberejerci cios	Compartic. amenazas	Servicio Preventivo

Especialización en diversos sectores

3 Fases implementadas

1. Ataque continuado
2. Roleplay
3. Simulación de incidente

Respuesta incidentes	Detección proactiva	Alerta temprana	Detector incidentes	Informatio n gathering	Ciberejerci cios	Compartic. amenazas	Servicio Preventivo

Compartir los IOC del malware conocido para facilitar la detección

- Anonimización de la información compartida
- Nodos de entrada para alimentación
- Nodos de salida para obtención de información
- Análisis y enriquecimiento de la información por parte de CERTSI

Compartición de amenazas

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Malspam 2017-09-20 "New voice message in mailbox" Locky...

Event ID	5783
Uuid	59c3812d-0d64-4d2f-886f-717fc0a80a8e
Org	INCIBE
Contributors	
Email	antonio.rodriguez@incibe.es
Tags	tlp:white x circl:incident-classification="malware" x malware_classification:malware-category="Ransomware" x +
Date	2017-09-20
Threat Level	Low
Analysis	Completed
Distribution	All communities
Info	Malspam 2017-09-20 "New voice message in mailbox" Locky ransomware (.ykcol)
Published	Yes

Pivots | Attributes | Discussion

5783: Malspa...

« previous | 1 | 2 | 3 | next » | view all

Related Events

2017-09-26 (5813) 2017-09-22 (5801) 2017-09-18 (5778) 2017-09-14 (5769) 2017-09-12 (5760)

2017-09-12 (5765) 2017-08-28 (5668) 2017-03-27 (3974) 2016-04-14 (2359) 2016-03-17 (2206)

Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Include deleted attributes | Show context fields

Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2017-09-21		Payload delivery	filename	IM<10 digits>.vbs	Malicious vbs		No	Inherit	
2017-09-21		Payload delivery	filename|sha1	IM2220386274.vbs | 91acc61f49d7164fdd22679b8059259001c1e39e	Malicious file embedded on 7z		Yes	Inherit	
2017-09-21		Payload delivery	filename|sha1	IM2385631810.vbs | fc2eee58e3f62e0f7eeb1636df73ac6b110f6b8b	Malicious file embedded on 7z		Yes	Inherit	
2017-09-21		Payload delivery	filename|sha1	IM2462942009.vbs | c19d1f10bd3b286eff5a0b9bc3423b7c7f801192	Malicious file embedded on 7z		Yes	Inherit	
2017-09-21		Payload delivery	filename|sha1	IM309182939.vbs | e2065ddb0e108d6495fde5faba3f16960b8a92b3	Malicious file embedded on 7z		Yes	Inherit	
2017-09-21		Payload delivery	filename|sha1	IM3213319504.vbs | 5a21e54cd506fd477c5389c3983b89c972816824	Malicious file embedded on 7z		Yes	Inherit	
2017-09-21		Payload delivery	filename|sha1	IM3314020470.vbs | e1f002079f4eff22aed4d9cf0bed0e13953144ae	Malicious file embedded on 7z		Yes	Inherit	
2017-09-21		Payload delivery	filename|sha1	IM3314884265.vbs | b49bd627f7187f35794999ec050904e7c30ec8b9	Malicious file embedded on 7z		Yes	Inherit	

Compartición de amenazas

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Event ID	5788
Uuid	59c4f605-6cf0-4081-93c7-7aeec0a80a8e
Org	INCIBE
Contributors	
Email	icaro@incibe.es
Tags	tlp:green x certsi:critical-sector="financial" x circl:incident-classification="malware" x malware_classification:malware-category="Trojan" x +
Date	2017-09-21
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	Cobalt Strike attack on banks' infrastructure using "CVE-2017-8759" 20-21 September
Published	Yes

Pivots | Attributes | Discussion

5788: Cobalt...

« previous | next » | view all

Related Events

2017-09-25 (5807) 2017-09-22 (5787) 2017-07-11 (5544) 2017-07-07 (5541) 2017-07-03 (5509)
2017-06-27 (5507) 2015-11-19 (1837) 2015-09-08 (1619) 2015-09-08 (1620) 2015-09-08 (1621)
2015-09-03 (1600) 2015-02-18 (853) 2015-02-17 (846) 2015-02-16 (841) 2015-02-16 (845)
2014-12-22 (745) 2014-11-05 (631) 2014-11-04 (629)

Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Include deleted attributes | Show context fields

Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2017-09-22		Attribution	threat-actor	Carbanak		1837 1621 1620 1619 1600 853 846 845 841 745 631 629	No	Inherit	
2017-09-22		External analysis	comment	Report produced by BI.ZONE CERT			No	Inherit	
2017-09-22		External analysis	text	On September 20 and 21 threat actors from Carbanak cybergang conducted new phishing attack. Phishing e-mails contain malicious document in RTF format (".doc") with the link to XML-file located on the external source (in this particular case, the name of the file is "test.xml"). This file embodies malicious code that exploits vulnerability "CVE-2017-8759" (WSDL Parser Code Injection). Once the vulnerability is exploited, Cobalt Strike Beacon software is downloaded to the system through the execution of malicious code .NET. Upon the download and start of the malicious software, threat actors get full access to the infected system.		No	Inherit	
2017-09-22		External analysis	vulnerability	CVE-2017-8759			No	Inherit	

Compartición de amenazas

Ataque a compañías del sector energético

Event ID	5564
Uuid	59706421-ea60-4956-a2d3-6f06c0a80a8e
Org	INCIBE
Contributors	
Email	javier.berciano@incibe.es
Tags	tlp:amber x certsi:critical-sector="energy" x circl:incident-classification="malware" x +
Date	2017-07-20
Threat Level	High
Analysis	Ongoing
Distribution	Operadores
Info	Ataque a compañías del sector energético
Published	Yes

Pivots Attributes Discussion

5564: Ataque...

« previous next » view all

Related Events

2017-09-06 (5731) 2017-07-07 (5524) 2016-12-29 (3621)

Filters: All File Network Financial Proposal Correlation Warnings Include deleted attributes Show context fields

Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2017-09-20		Network activity	domain	mail.devangeconstruction.com			Yes	Inherit	
2017-07-20		Network activity	ip-dst	5.153.58.45	Direcciones IP involucradas	5524	Yes	Inherit	
2017-07-20		Network activity	ip-dst	62.8.193.206	Direcciones IP involucradas	5524	Yes	Inherit	
2017-07-20		Network activity	ip-dst	184.154.150.66	Direcciones IP involucradas	5731 5524	Yes	Inherit	
2017-07-20		Network activity	ip-dst	185.22.184.71	Direcciones IP involucradas		Yes	Inherit	
2017-07-20		Network activity	ip-dst	85.159.65.114	Direcciones IP involucradas		Yes	Inherit	
2017-07-20		Network activity	ip-dst	187.130.251.249	Direcciones IP involucradas		Yes	Inherit	
2017-07-20		Network activity	ip-dst	167.114.44.147	Direcciones IP involucradas		Yes	Inherit	

Servicios del CERT

Respuesta incidentes	Detección proactiva	Alerta temprana	Detector incidentes	Informatio n gathering	Ciberejerci cios	Compartic. amenazas	Servicio Preventivo

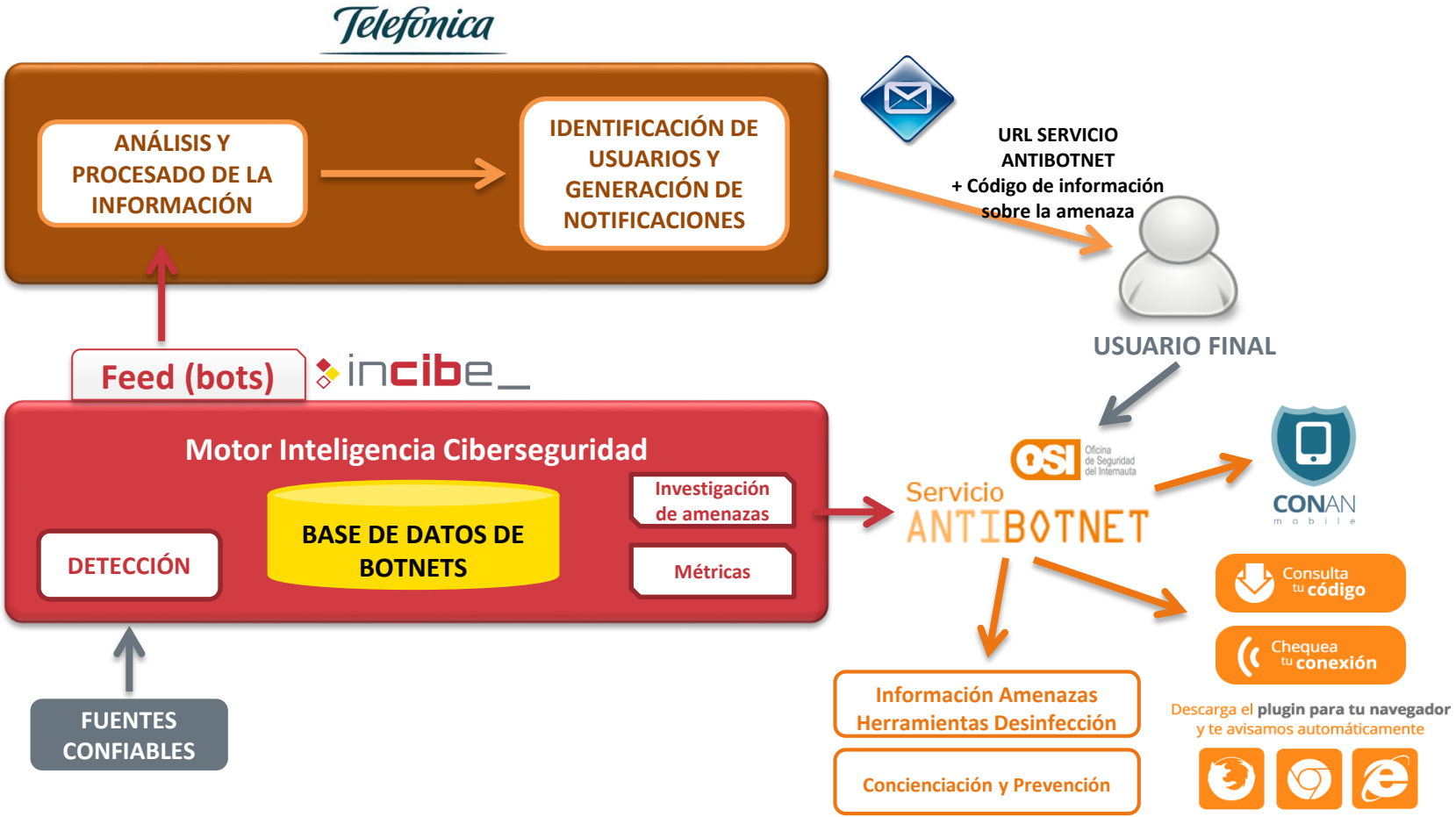
Aprovechar el conocimiento adquirido para proteger

- Estudios
- Guías
- Hojas de referencia
- Buenas prácticas

Más de **10 millones de eventos diarios** relacionados con conexiones a servidores de control de botnets

900 sinkhole externos que permiten monitorizar más de **130 botnets**

Servicio AntiBotnet



Servicio AntiBotnet

Servicio
ANTIBOTNET

Servicio chequeo online permite comprobación desde cualquier navegador

Conan mobile aplicación Android para comprobar nivel de seguridad del dispositivo móvil

Plugin para principales navegadores, con alertas personalizables

Notificación del ISP diariamente Telefónica reporta a los clientes las posibles infecciones

API para empresas que permite comprobación automática e integración en sus sistemas de seguridad

Síguenos en…

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

CONTACTO	**Instituto Nacional de Ciberseguridad (INCIBE)** info@incibe.es
VISÍTANOS	**Instituto Nacional de Ciberseguridad (INCIBE)** https://www.incibe.es
INFÓRMATE	**CERT de Seguridad e Industria (CERTSI)** https://www.certsi.es **Oficina de Seguridad del Internauta (OSI)** https://www.osi.es **CyberCamp** https://www.cybercamp.es **Internet Segura for Kids** https://www.is4k.es/
SÍGUENOS	**Twitter, YouTube, Facebook, LinkedIn, G+.** @Incibe @Certsi_ @Osiseguridad @is4kids @CyberCampEs @CiberEmprende_
REPÓRTANOS	**Incidentes, vulnerabilidades, fraude online, phishing, malware, etc.** incidencias@certsi.es y consultas@osi.es