Servicios a la comunidad de RedIris

INCIBE-CERT

Francisco A. Lago García
Responsable Servicios Avanzados INCIBE-CERT

GOBIERNO DE ESPAÑA
MINISTERIO DE ECONOMÍA Y EMPRESA

www.incibe.es

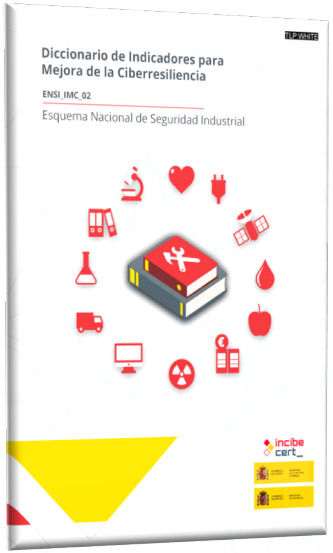
INSTITUTO NACIONAL DE CIBERSEGURIDAD

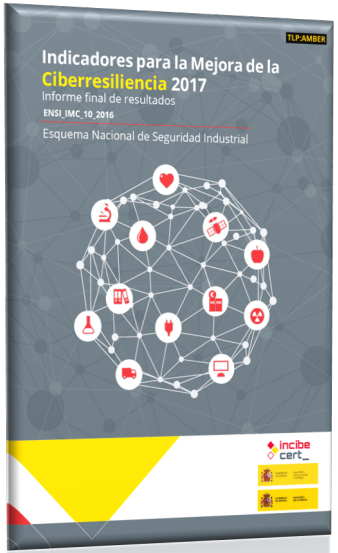
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe-cert_

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Medición de la Ciberresiliencia





¿Qué es la metodología de medición de indicadores de ciberresiliencia?

La Ciberresiliencia se define como la capacidad de **anticipar, resistir, recuperarse y evolucionar** para sobreponerse a condiciones adversas (como los ataques contra los recursos de información o tecnológicos).

Los Indicadores para la Mejora de la Ciberresiliencia (IMC) son un instrumento de diagnóstico y medición de la capacidad de las organizaciones para soportar y sobreponerse a desastres y perturbaciones procedentes del ámbito digital.

2014
Ciberresiliencia

2015
PILOTO IMC
31 Operadores

2016
ENSI
Esquema Nacional de Seguridad Industrial para Operadores Críticos

2017
PILOTO IMC
128 Operadores

ANTICIPAR:
Mantener un estado de preparación informado, con el fin de evitar compromisos de funciones misión / empresa de los ciberataques

RESISTIR:
Continuar las funciones críticas a pesar de la ejecución con éxito de un ciberataque.

RECUPERAR:
Restaurar las funciones críticas en la mayor medida posible con posterioridad a la ejecución con éxito de un ciberataque.

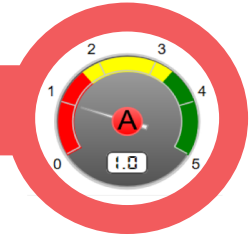
EVOLUCIONAR:
Cambiar misiones, funciones y capacidades cibernéticas de apoyo, a fin de minimizar los impactos negativos de los ciberataques.

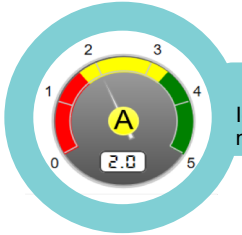
Metodología Medición de Ciberresiliencia

OBJETIVOS

Conocer el nivel de madurez

Capacidad de la organización en ciberresileincia, para hacer frente y resistir a ataques contra sus sistemas de información o de operación



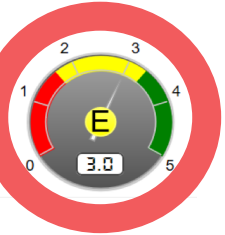


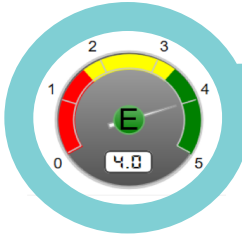
Mejorar la ciberresiliencia

Identificar los dominios funcionales de seguridad que podrían ser mejorados en la organización, mediante un plan de acción adecuado

Revisión Continua

Disponer de un marco de revisión que permita una autoevaluación periódica para la mejora continua de la seguridad de la organización





Comparación de resultados

Facilitar la comparación de resultados frente a otras organizaciones del mismo sector y entorno tecnológico

Metodología Medición de Ciberresiliencia

Las 46 métricas de la consulta se agrupan jerárquicamente en:

- ❑ **Entornos tecnológicos** a proteger. Diferenciando entre entornos IT u OT (sistemas industriales, SCADA o ICS).
- ❑ **Metas objeto** a alcanzar.
- ❑ Categorías o **dominios funcionales de ciberresiliencia** a implantar.

Niveles de madurez	
L0	**INEXISTENTE**: Esta medida no está siendo aplicada en este momento.
L1	**INICIAL / AD-HOC**: Cuando la organización no proporciona un entorno estable. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas. Pese a un naturaleza caótica, es más que no tener nada; pero es difícil prever la reacción ante una situación de emergencia.
L2	**REPETIBLE, pero INTUITIVO**: Cuando existe un mínimo de planificación que, acompañada de la buena voluntad de las personas proporciona una pauta a seguir cuando se repiten las mismas circunstancias. Es impredecible el resultado si se dan circunstancias nuevas.
L3	**PROCESO DEFINIDO**: Se dispone un catálogo de procesos que se mantiene actualizado. Estos procesos garantizan la consistencia de las actuaciones entre las diferentes partes de la organización, que adaptan sus procesos particulares al proceso general.
L4	**GESTIONADO Y MEDIBLE**: Cuando se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.
L5	**OPTIMIZADO**: En este nivel la organización es capaz de mejorar el desempeño de los sistemas a base de una mejora continua de los procesos basada en los resultados de las medidas e indicadores.

Metodología Medición de Ciberresiliencia

46 MÉTRICAS DE CIBERRESILIENCIA

9 ANTICIPAR

- POLÍTICA DE CIBERSEGURIDAD — 3
- GESTIÓN DE RIESGOS — 4
- FORMACIÓN EN CIBERSEGURIDAD — 2

13 RESISTIR

- GESTIÓN DE VULNERABILIDADES — 9
- SUPERVISIÓN CONTINUA — 4

20 RECUPERAR

- GESTIÓN DE INCIDENTES — 9
- GESTIÓN DE CONTINUIDAD DEL SERVICIO — 11

4 EVOLUCIONAR

- GESTIÓN DE LA CONFIGURACIÓN Y DE LOS CAMBIOS — 1
- COMUNICACIÓN — 3

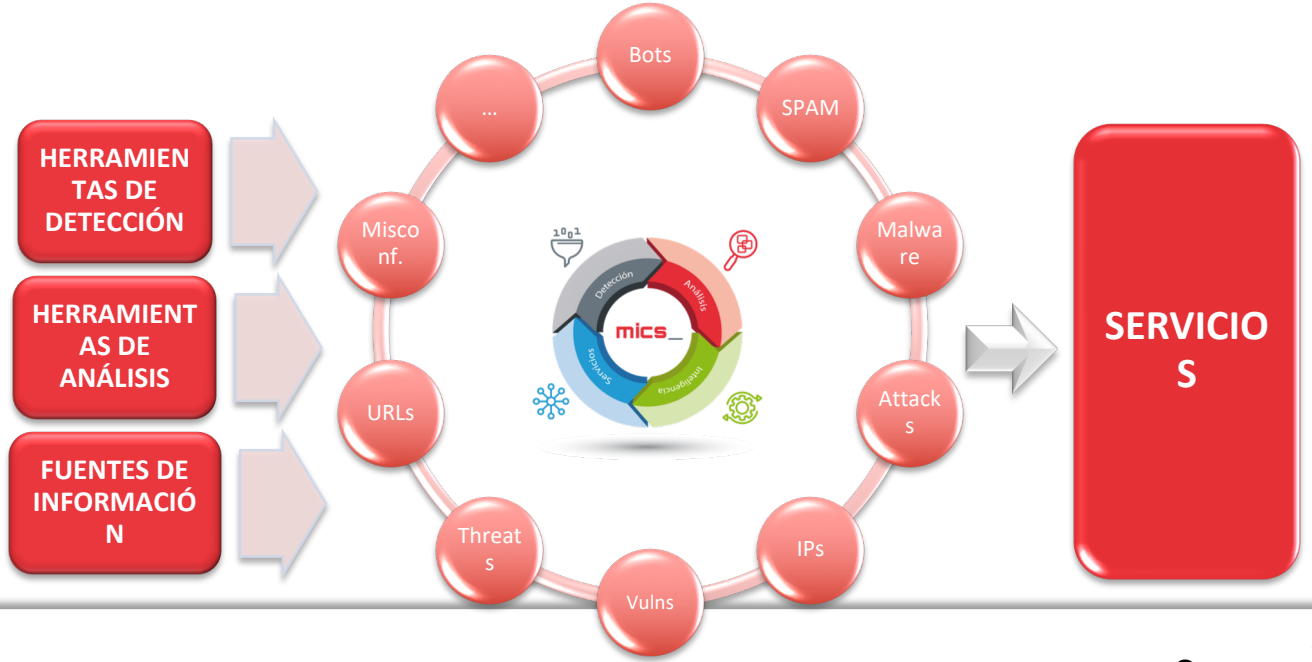
Lanzamiento del servicio

- **Más información:** https://www.incibe-cert.es/publicaciones/ensi/ensi_imc
- **Piloto con 40 entidades de RedIris: ICTS, Redes Regionales, Universidades** (CRUE Seg.)
- **Proyecto bianual (2019 y 2020): 2 mediciones, inicial y final. Comparativa y evolución**
- Inscripciones: seguridad@rediris.es

Monitorización de Activos

Modelo de Inteligencia en Ciberseguridad

- **MICS:** Sistema BIG Data y Correlación de eventos de seguridad. 50 Tipos eventos: Bots, Sistemas expuestos/vulnerables, SPAM, Phising, Malware, Ataques, Configuraciones inseguras, …
- Media de **eventos diarios** procesados**: >15.000.000**
- Número de **activos** únicos **(Mayo): >3.800.000**
- **Herramientas propias de detección:** amenazas, sistemas expuestos o vulnerables, etc
- Número de **fuentes: 30**



Monitorización de Activos: Servicio y lanzamiento

- Identificación de **Activos de la Entidad**
  - ✓ **IPs** públicas
  - ✓ **Dominios** publicados en Internet
- Identificación de **contactos de la Entidad**
  - **Nivel 0, 1 y 2** (Institucional, Notificación Incidentes, Responsable Ciberseguridad)
- Lanzamiento **piloto** con ICTS en 2019
- Progresivamente se irá abriendo a otras entidades interesadas de RedIris
- Inscripciones: seguridad@rediris.es


icaro_
MISP
Threat Sharing
IP
EVENT A
EVENT B
Database
API
MISP XML and JSON
OpenIOC
STIX XML and JSON (export)
Suricata export
Snort export
CSV export
GFI import

Ícaro: Repaso

- **Compartir información de inteligencia sobre amenazas:** IOCs, análisis, información de fraude, información de vulnerabilidades, etc. **Herramienta de análisis**
- **Automatización: sincronización** con otros MISP. **Información estructurada. Importación y exportación** en varios formatos.
- **Integración con otras herramientas: API**
  - ✓ IDS (Snort, Suricata, Bro/Zeek)
  - ✓ Splunk
  - ✓ VirusTotal, Joe Sandbox
  - ✓ The Hive, Cortex
  - ✓ Endpoint: p.e. Mcafee Active Response
  - ✓ ....
- **¿Por qué ÍCARO? MISP vitaminado**
  - Acceso a **fuentes privadas** de INCIBE: + Información y privilegiada
  - **Operación INCIBE**: eventos propios, revisión de fuentes, actualización, filtrado, …

Ícaro: Repaso

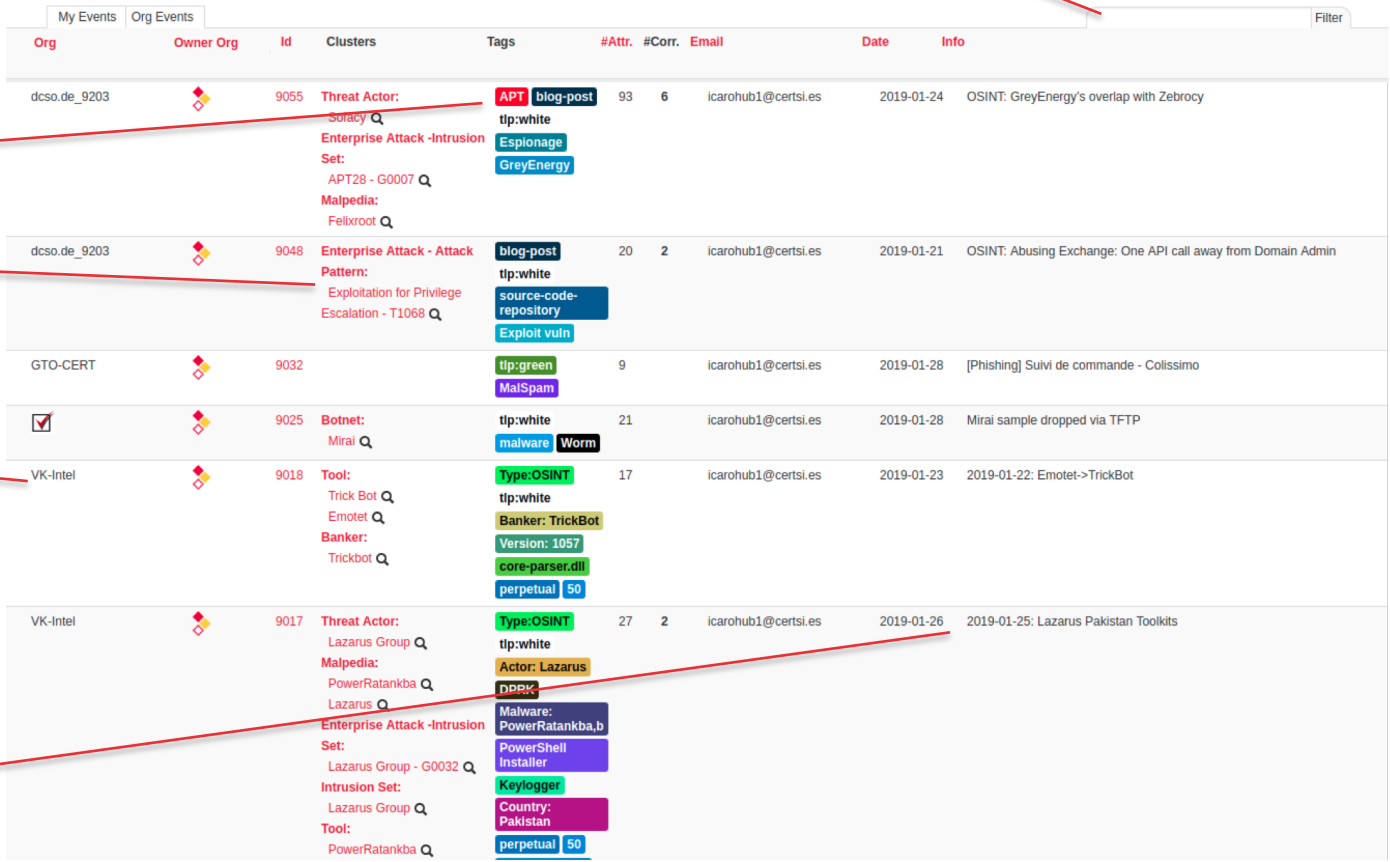
Búsqueda: texto, IPs, hash, dominio, url …

Etiquetas

Galaxias

Entidad autora del evento

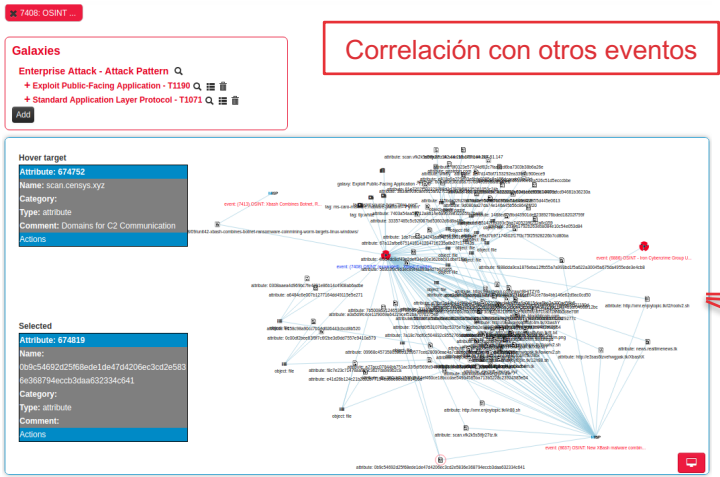
Fecha y descripción del evento



Ícaro: Repaso

Análisis: documentación, enlaces, gráficos, etc.

Correlación con otros eventos



Date ↑	Org	Category	Type	Value	Comment	Correlate	Related Events	Feed hits	IDS	Distribution
2017-05-19		External analysis	attachment		WannaCry schema	☑			No	Inherit
2017-05-19		External analysis	attachment	inThreat Flash Intel #10 - Ransomware Worm WannaCry.pdf	WannaCry analysis	☑			No	Inherit
2017-05-19		External analysis	attachment	20170515_Wannacrypt.mtgl	WannaCry maltego	☑			No	Inherit
2017-05-16		External analysis	vulnerability	CVE-2017-0145	ETERNALBLUE	☑	8327		No	All
2017-05-16		Payload delivery	sha256	1b974d46cde9f6e837ec369120dd2727eb774ca58fa8d552b9baeb2c411b0cdc	Wannacry variant with ETERNALBLUE Exploit (VT search)	☑	5249		Yes	Inherit
2017-05-16		Payload delivery	sha256	fe4a98768de3aad02a56de713c57962b33719776d6aa694cd11f0590828abd33	Wannacry variant with ETERNALBLUE Exploit (VT search)	☑	5249		Yes	Inherit
2017-05-16		Payload delivery	sha256	0db91ff8822f1623fe36d712b5f56d339dc21008f1ecc617a5de2f522039c5b3	Wannacry variant with ETERNALBLUE Exploit (VT search)	☑	5254 5249		Yes	Inherit
2019-01-04		Network activity	hostname	asthma.weilders.com	Other Network Activity	☑	8269		Yes	Inherit
2019-01-04		Network activity	ip-dst	207.148.110.212	Other Network	☑	8269			

Indicadores de compromiso.
Accionables (IDS, otras herramientas ...)

Actualizaciones del Servicio

- **Formación: Curso Uso, Operación y Administración MISP. RedIris. Madrid. 17-18/09**
  - Inscripciones: seguridad@rediris.es
- Redefinición arquitectura para servicio a Comunidad RedIris
- Más Información: icaro@incibe.es - Próximamente buzón de RedIris

Gracias por su atención