Infraestructuras Criticas

Pasado, presente y futuro

PhD. Luis Enrique Sánchez Crespo.

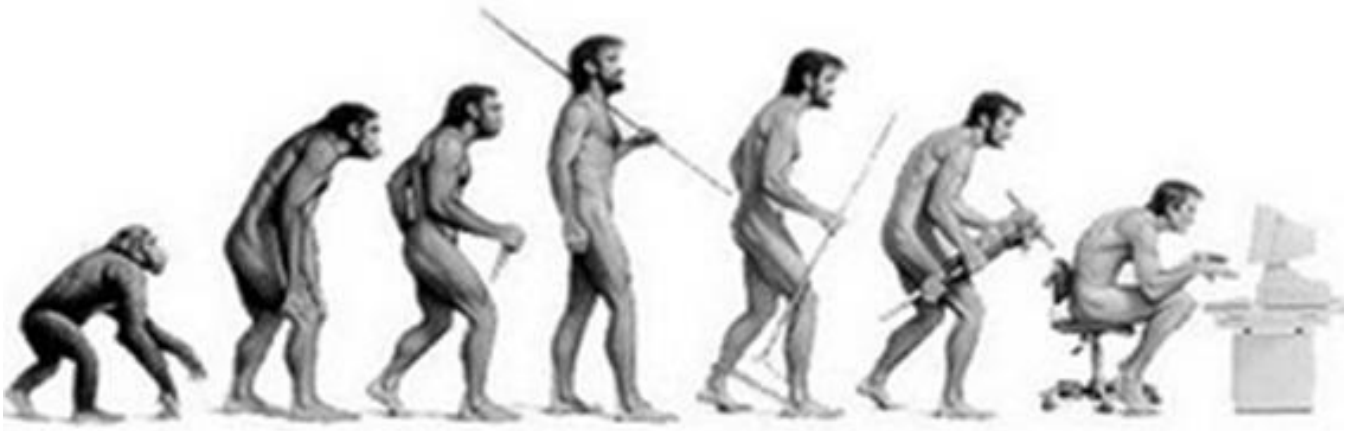
Experto en Ciberseguridad - Universidad Castilla-la Mancha.

UCLM UNIVERSIDAD DE CASTILLA-LA MANCHA · GSyA Grupo de Investigación en Seguridad y Auditoría · SICAMAN · MARISMA

¿Cómo hemos llegado a la situación actual?

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA
GSyA
Grupo de Investigación en Seguridad y Auditoría
SICAMAN
MARISMA

En 1995 entramos en una nueva etapa…



…La era del **Conocimiento**

Esta nueva etapa trajo **grandes ventajas** …

…Pero también **grandes riesgos**.

Y el mundo se vio enfrentado a **tres grandes amenazas:**

- Cibercrimen.

- Ciberterrorismo.

- Ciberguerra.

CiberArmas

La industria marítima es presa fácil para los cibercriminales

KASPERSKY DAILY

22 May 2015

cer más uso de los sistemas
ca que de sus propias
enor a medida que se utilizan
anipulación y el seguimiento de
mbién son muy vulnerables a

Los investigadores han descubierto agujeros de seguridad en las tecnologías clave de las embarcaciones: en el GPS, el Sistema de Identificación Automática (AIS) marina y en el Sistema de Información y Visualización de la Carta Electrónica (ECDIS). Otro problema es que en caso de que haya un dispositivo vulnerable a bordo, la mayoría de la tripulación no está preparada para afrontar una situación como ésta. Por ejemplo, el hackeo de un GPS podría mandar al barco por otra ruta y hacer que éste siguiera apareciendo en su ruta correcta. Esto podría provocar una colisión y un retraso del reparto de la mercancía.

En 2010, movieron una torre de perforación de su sitio de construcción en Corea del Sur hacia Sudamérica. Los ordenadores y sistemas de control de las embarcaciones se llenaron de virus. Llevó 19 días identificarlo y arreglarlo. Hubo otros incidentes similares incluyendo el que reportó Reuters recientemente. Se tuvo que cerrar una plataforma petrolera flotante durante una semana hasta que se solucionara el problema porque no había profesionales en ciberseguridad a bordo.

LUNES, 23 DE MAYO 2016, 16:03:50

La historia de los narcos mexicanos que hackearon el puerto de Amberes

Forbes MEXICO

Magal S3, una agencia de seguridad de Israel, recuerda en un reporte que una organización criminal comenzó a usar el puerto de Amberes para introducir drogas en cargamentos que supuestamente eran plátanos provenientes de Sudamérica.

El hackeo permitió a la organización criminal localizar cada contenedor, incluso antes de que el cliente real apareciera para reclamarlo. Detectaban su cargamento de drogas y lo movían a su antojo a través de la puerta de Europa.

El Confidencial

Así es como un ciberataque deja toda una ciudad a oscuras

El gobierno de Ucrania señala a Rusia como responsable del apagón que sufrieron diversas centrales eléctricas del país, en un ataque con virus informáticos. Unas 80.000 personas se quedaron sin electricidad durante 6 largas horas, abandonadas al frío del 23 de diciembre de 2015. El mismo virus ha hecho saltar las alarmas hace unos días, al ser detectado en la red que controla el tráfico aéreo del aeropuerto de Ucrania.

El virus se llama **BlackEnergy** y es el primero en la historia —que conozcamos — involucrado en un apagón eléctrico generalizado. Antes que él, **Stuxnet**, obra de Israel y Estados Unidos, dañó seriamente diversas centrales nucleares iraníes, pero no dejó a nadie sin luz.

Pasado

elEconomista.es | Empresas y finanzas

Miércoles, 27 de Abril de 2016 Actualizado a las 17:29

Alemania reconoce que su planta nuclear más potente ha sido hackeada

EL PAÍS 12 MAY 2017 - 23:11 CEST

Un ciberataque paraliza 16 hospitales de Reino Unido y les exige dinero

RT SEPA MÁS

'Hackean' una planta potabilizadora y cambian la composición química del agua

Publicado: 27 mar 2016 17:23 GMT | Última actualización: 27 mar 2016 17:25 GMT

¿Realmente es rentable el ciber-crimen?

Norton™ by Symantec

"EL CIBERCRIMEN ES MÁS GRANDE QUE...

.....el mercado negro de **marihuana, cocaína y heroína** combinados (295 000 millones de dólares) en todo el mundo y se acerca al valor del **tráfico de drogas global** (411 000 millones de dólares). [i]

Con 388 000 millones de dólares, el cibercrimen supera más de **100 veces los gastos anuales de UNICEF** (3 650 millones de dólares). [ii]

¿Qué pasaría si todas esas infraestructuras criticas fueran atacadas a la vez por una nación hostil o por terroristas?

Caso Ilustrativo – Estonia 2007

A continuación se presenta cronológicamente, el ataque cibernético documentado más grande de la historia.

Abril 15

El Gobierno de Estonia, decide remover del centro de Tallin el Monumento del Soldado de Bronce, lo cuál genera un fuerte enfrentamiento diplomático con Rusia.

Abril 26

El ataque cibernético empezó a las 10 p.m.. Al final de esa primera semana, todas las páginas web gubernamentales y de los diferentes partidos políticos habían sido bloqueadas.

Mayo 2

La segunda semana, todos los medios de comunicación quedaron completamente desconectados, haciendo imposible que se le informara al mundo lo que estaba ocurriendo

Mayo 9

A medianoche, ocurrió el ataque más fuerte. Los hackers desconectaron todo el sistema bancario. bloquearon sus páginas web y los cajeros electrónicos dejaron de funcionar.

Mayo 15

Durante tres semanas, los sitios web del gobierno, los bancos, medios de comunicación y todas las universidades fueron sistemáticamente atacados y desconectados.

Mayo 19

Los ataques se detuvieron y la primera ciberguerra llegó a su fin. Estonia inmediatamente acusó al gobierno de Rusia, pero nada ha podido ser demostrado.

Conclusiones del Apartado

1. Nos enfrentamos a un nuevo mundo. Con nuevos retos. Un **mundo interconectado**, con más dispositivos autónomos, y que dependen cada vez más de la tecnologías.

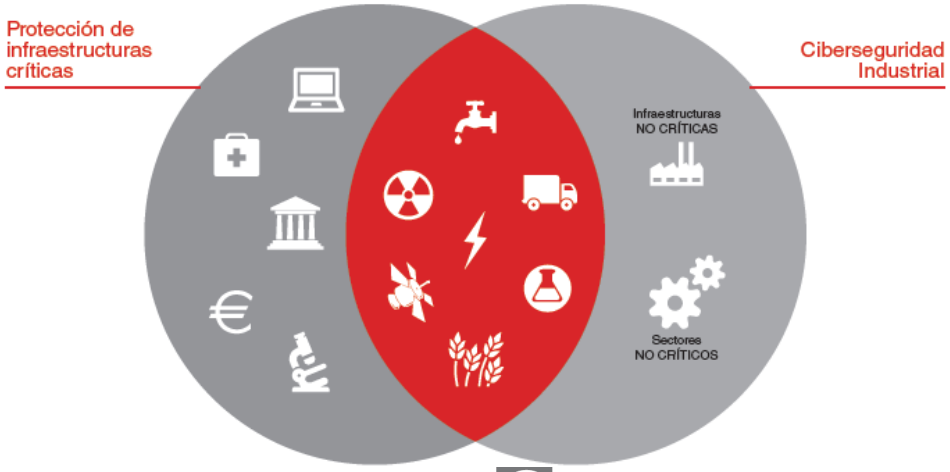
2. Pero con esos avances se han producido **grandes riesgos que deben ser controlados**.

3. Ese control empieza **identificando y protegiendo las infraestructuras criticas** de una nación.

¿Dónde nos encontramos actualmente?

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA
GSyA
Grupo de Investigación en Seguridad y Auditoría
SICAMAN
MARISMA

- Los acontecimientos ocurridos durante los últimos años (el 11S en 2001, actos de ciberespionaje, Anonymous, Wikileaks, Stuxnet, etc), han llevado a los gobiernos a incluir en sus agendas el **desarrollo de Estrategias Nacionales de Ciberseguridad** y medidas de protección para garantizar la **Seguridad de sus Infraestructuras Críticas (PIC)** y de sus **Infraestructuras Industriales (CI)**.



La Protección de Infraestructuras Críticas y la Ciberseguridad Industrial

Infraestructura Critica

- **Estados Unidos de América**, creo en el año ***1995*** la Directiva Presidencial numero 39 (PDD-39) US Policy on Counterterrorism.
- En **Europa** fue en ***2004*** cuando se creo la Agencia Europea de Seguridad de las Redes y de la Información (ENISA). Ese mismo año ***España creo el Real Decreto 421/2004***, de 12 de marzo, que demanda unos ***servicios de inteligencia eficaces, especializados y modernos***, capaces de afrontar los nuevos retos del actual Infraestructura Critica nacional e internacional.

enisa
European Network and Information Security Agency

CNPIC
CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

European Commission
MOBILITY AND TRANSPORT

Índice

MAPA DE RUTA
CIBERSEGURIDAD INDUSTRIAL
EN ESPAÑA 2013 - 2018

La Protección de Infraestructuras Críticas y la Ciberseguridad Industrial

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

GSyA
Grupo de Investigación en Seguridad y Auditoría

SICAMAN

MARISMA

¿Pero como saber cuales son o no Infraestructuras Criticas?

- Respondiendo a la pregunta: **¿Si yo quisiera colapsar la economía de una país, que empresas y en que sectores debería atacar?**
- Formalmente, las Infraestructuras Críticas son entidades que el **CNPIC** y la **Secretaría de Estado de Seguridad del Ministerio del Interior** consideran como **ESTRÁTEGICAS**, ya que **prestan servicios esenciales** a nuestra sociedad, pero cuya sustitución o reemplazo no presenta alternativa posible.

Actualmente se han agrupado en 12 los sectores para Infraestructuras Críticas, que están siendo abordados de forma gradual (BOE-A-2011-7630).

Sector	Ministerio/Organismo del sistema
Administración.	Ministerio Presidencia.
	Ministerio Interior.
	Ministerio Defensa.
	Centro Nacional de Inteligencia.
	Ministerio Política Territorial y Administración Pública.
Espacio.	Ministerio Defensa.
Industria nuclear.	Ministerio Industria, Turismo y Comercio.
	Consejo de Seguridad Nuclear.
Industria química.	Ministerio Interior.
Instalaciones de investigación.	Ministerio Ciencia e Innovación.
	Ministerio Medio Ambiente, y Medio Rural y Marino.
Agua.	Ministerio Medio Ambiente, y Medio Rural y Marino.
	Ministerio Sanidad, Política Social e Igualdad.
Energía.	Ministerio Industria, Turismo y Comercio.
Salud.	Ministerio Sanidad, Política Social e Igualdad.
	Ministerio Ciencia e Innovación.
Tecnologías de la Información y las Comunicaciones (TIC).	Ministerio Industria, Turismo y Comercio.
	Ministerio Defensa.
	Centro Nacional de Inteligencia.
	Ministerio Ciencia e Innovación.
	Ministerio Política Territorial y Administración Pública.
Transporte.	Ministerio Fomento.
Alimentación.	Ministerio Medio Ambiente, y Medio Rural y Marino.
	Ministerio Sanidad, Política Social e Igualdad.
	Ministerio Industria, Turismo y Comercio.
Sistema financiero y tributario.	Ministerio Economía y Hacienda.

¿Qué implica ser infraestructura critica?

- La designación de un operador como crítico conlleva la **OBLIGACIÓN de desarrollar una planificación donde se plasmen las políticas de seguridad, metodologías y análisis de riesgos que permitan la protección de unos activos que son especialmente importantes para la prestación de servicios esenciales para la sociedad.**

Plan de Seguridad del Operador (PSO)

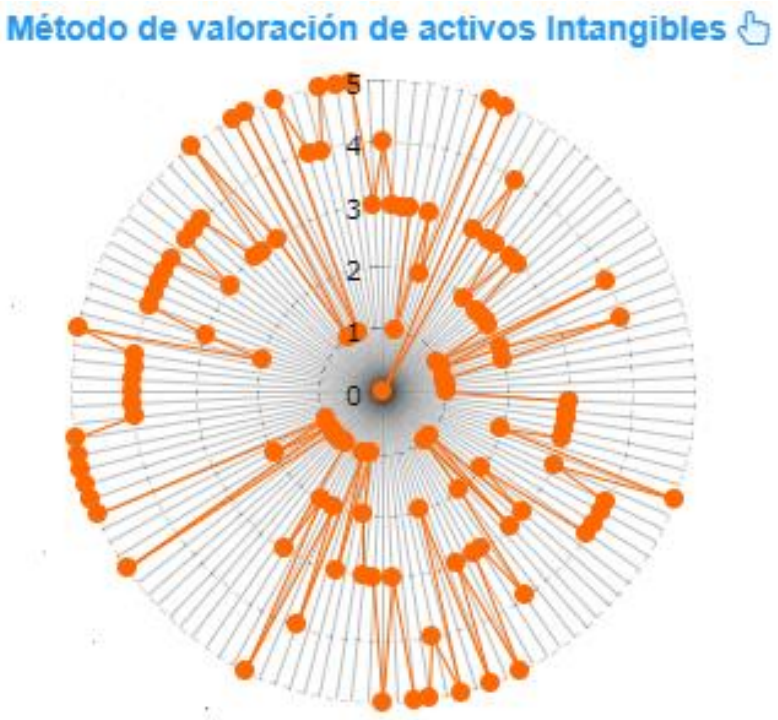
- Documento estratégico donde se recogerán las políticas generales de los operadores críticos, la ***metodología seguida para el análisis de riesgos*** y el criterio que se va a seguir para la aplicación de medidas de seguridad adecuadas.
- El objetivo del PSO es poder llegar a garantizar la seguridad o la gestión del conjunto de instalaciones o sistemas de su propiedad.
- También debe incluir ***aspectos formativos y de concienciación*** que se lleven a cabo para reforzar este plan de seguridad.

Plan de Protección Especifico (PPE)

- Engloba los documentos catalogados como operativos. En él se deben definir las **medidas concretas** tanto existentes, como las que se vayan a adoptar por los operadores críticos.
- Debe incluir un ***análisis de riesgos*** junto con la metodología marcada por nuestro PSO. Así, Obtendremos una criticidad por activo y podremos pasar a gestionar el riesgo de una forma más efectiva.
- Debe incluir el ***Plan de acción***.

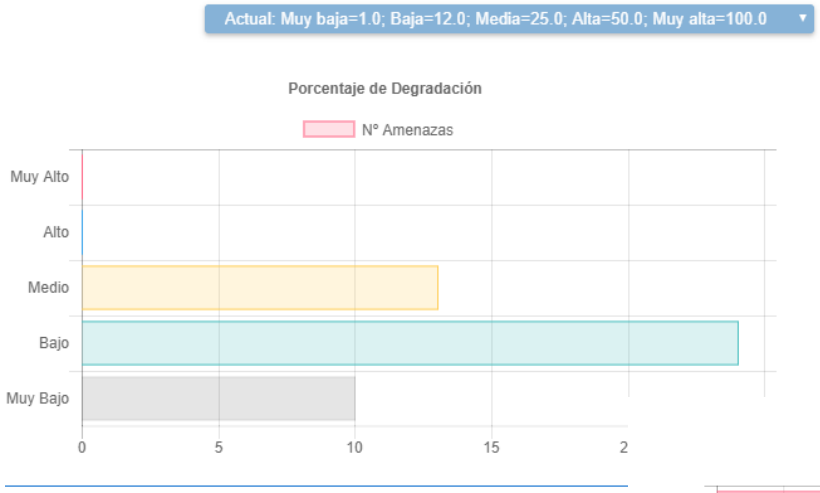
Análisis del Riesgo

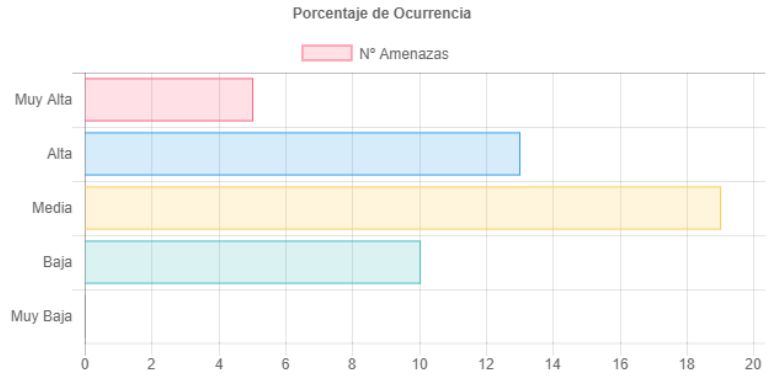
- Identificando los activos: Entre 100-300 activos de grano grueso con valoración cualitativa.



Análisis del Riesgo

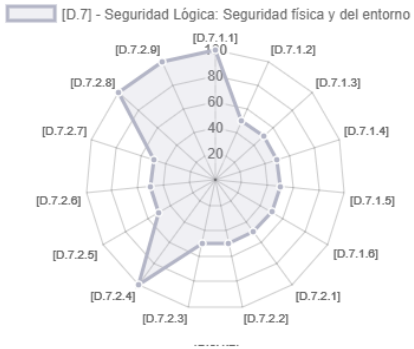
- Identificando de amenazas: 47 amenazas.

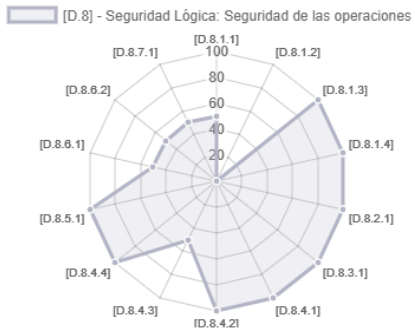




Análisis del Riesgo

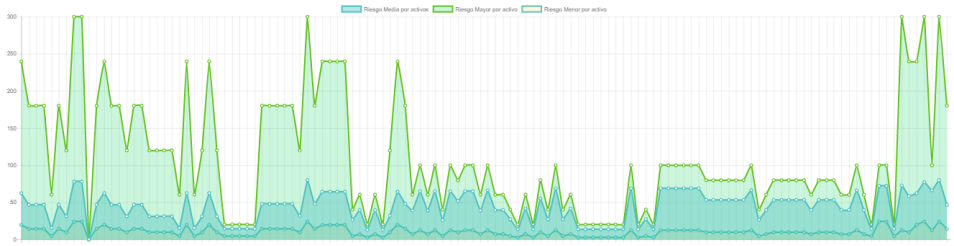
- Identificación Controles/Salvaguardas: Más de 300 controles de seguridad física y lógica.



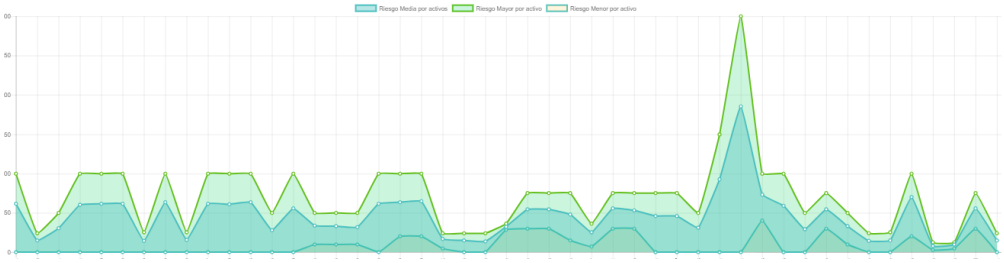


Análisis del Riesgo

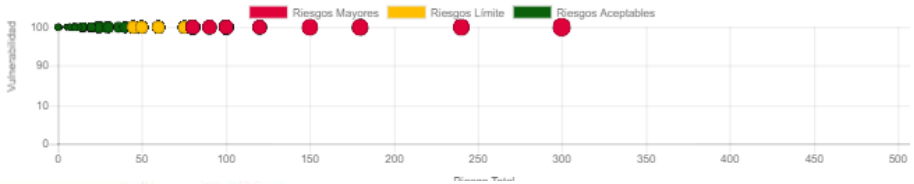
- Nivel de riesgo por activo.



- Nivel de riesgo por amenaza.



- Mapas de riesgos.



Plan de Acción

- Medidas especificas según nivel de alerta.

Gestión de la información, comunicaciones y operaciones								
Cultura de la Seguridad	Realización de boletines de seguridad para informar a los usuarios.	1	2	3	4	5	CISO	Implantado
	Realización periódica de cursos de ciberseguridad a los usuarios para crear conciencia de ciberseguridad.	1	2	3	4	5	CISO	31/12/2018
	Implantar un sistema de medición de cultura de la seguridad que mediante el uso de checklist e ingeniería social mida de forma continua el nivel de cultura de seguridad de la empresa.	1	2	3	4	5	CISO	31/12/2018
	Valorar la implantación de normas relacionadas con la ciberseguridad (ISO27001, COBIT, ...)	1	2	3	4	5	CISO	31/12/2018
Segregación de redes	Segregar las redes para limitar el impacto de una amenaza	1	2	3	4	5	CISO	31/12/2018
Controlar las capacidades de los servidores críticos	Controlar las capacidades de los servidores críticos para evitar sobrecargarlos.	1	2	3	4	5	CISO	31/12/2018
	Comparar las capacidades de los servidores críticos con los históricos para detectar anomalías en su funcionamiento.	1	2	3	4	5	CISO	31/12/2018
Establecer un protocolo de respuesta inmediata ante	El CISO comunicará al CERTSI cualquier alerta relevante que se produzca.				4	5	CISO	Implantado
	El CISO comunicará al CERTSI cualquier alerta que se produzca.					5	CISO	Implantado
Restringir el acceso a la red	Bloquear las comunicaciones o cualquier acción informática que pueda tener acceso a la red y que no fuera totalmente imprescindible para la realización de las funciones de servicio de la empresa.					5	CISO	31/12/2018
Revisión de Vulnerabilidades	Realización de pruebas de pentesting anuales	1	2	3	4		CISO	31/12/2018
	Realización de pruebas adicionales de pentesting trimestrales.					5	CISO	31/12/2017

Niveles de Alerta

- Nivel de alerta el día 28-08-2017.

Conclusiones del Apartado

1. El nivel inicial de las Infraestructuras Criticas evaluadas es de entre un 60-75%, con unos 200 activos de grano grueso de media y un nivel de madurez medio-alto.
2. Estas compañías se enfrentan a retos como la falta de madurez de los modelos metodológicos y la falta de herramientas adecuadas.
3. Existe un alto nivel de concienciación y predisposición a implantar sistemas de seguridad y a realizar una correcta gestión de los mismos.
4. Se debe tener especial cuidado con las medidas propuestas, dado que el nivel de alerta esta la mayor parte del tiempo en 3-4, lo que puede hacer que un exceso de medidas bloquee la operativa de las empresas.

¿Hacia donde vamos?

Análisis del Riesgo. Problemas

- A lo largo de 20 años se ha ido analizando, investigando mediante el método científico investigación-acción y descubriendo fallos de los modelos existentes, los cuales se han ido transmitiéndose de unas normativas a otras.

- La investigación dentro del campo de la Gestión de la Seguridad y el Análisis de Riesgos, ha sido una de las principales líneas de investigación de GSyA las dos últimas décadas.

Para esta investigación, se ha buscado alinear todos los grupos de actores que tienen algo que decir dentro de la protección de la Infraestructuras Criticas y la Gestión de la Seguridad.

Instituciones Públicas

enisa European Network and Information Security Agency

CNPIC CENTRO NACIONAL PARA LA PROTECCIÓN DE LAS INFRAESTRUCTURAS CRÍTICAS

Universidades

UCLM UNIVERSIDAD DE CASTILLA-LA MANCHA

GSyA Grupo de Investigación en Seguridad y Auditoría

Empresas

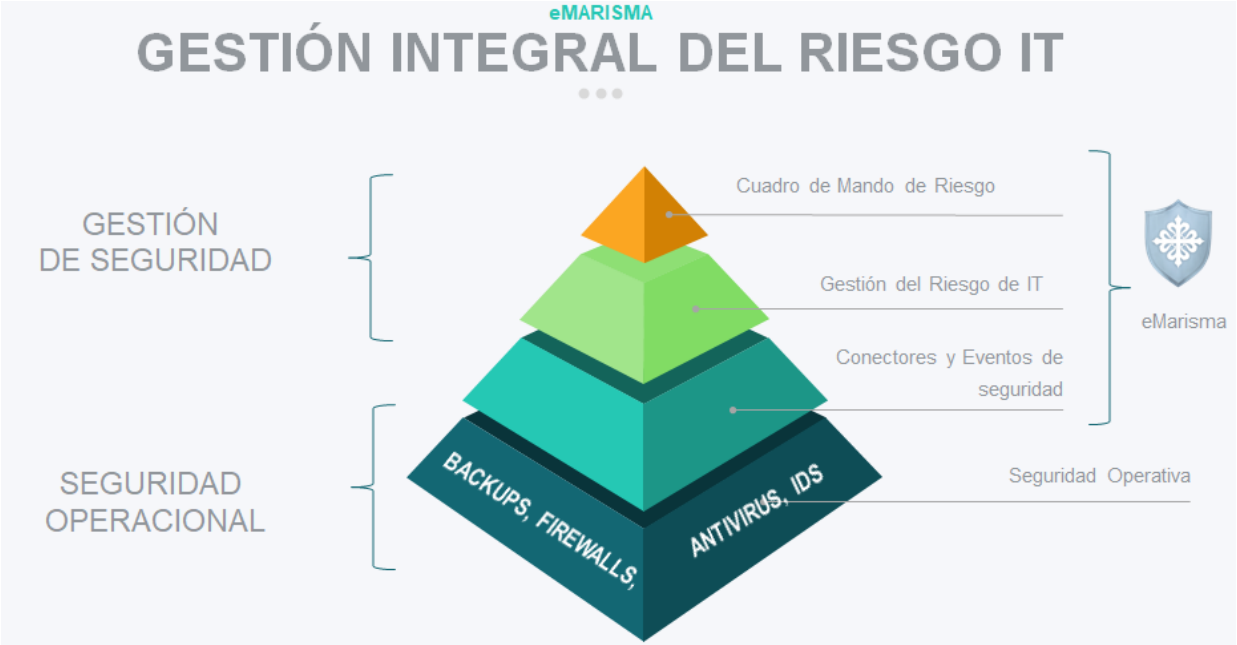
SICAMAN

COMISMAR TEC

grupo in-nova

Análisis del Riesgo. Problemas

- Fruto de estas investigaciones nace **MARISMA** (Metodología Análisis de Riesgos), que busca solucionar algunos de los problemas detectados y dar garantías de futuro dentro de las Infraestructura Criticas.



eMARISMA

Funcionalidades

Informe Previo

Informe de análisis
Plan de tratamiento

Indicadores

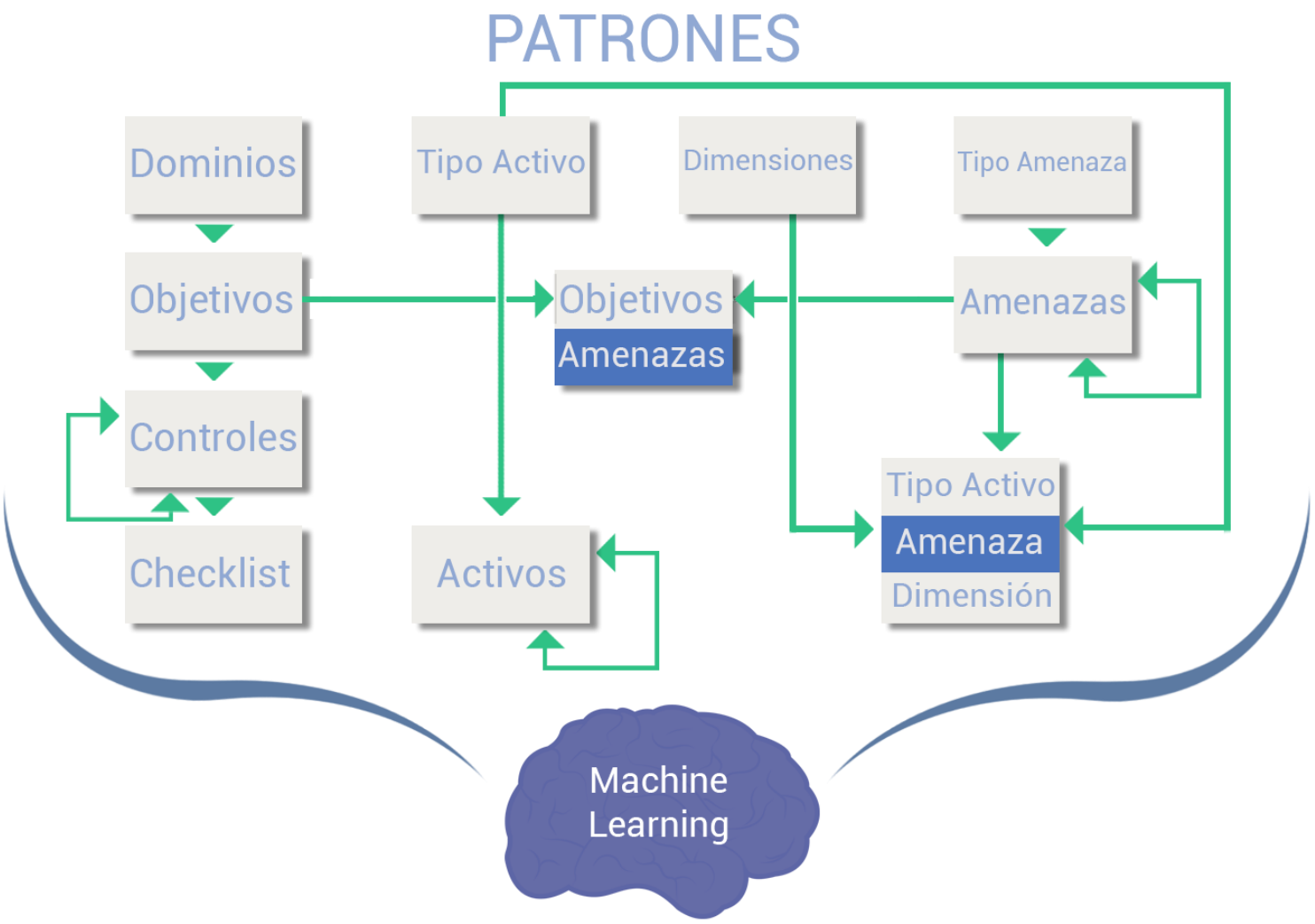
PREAUDITORÍA | GESTIÓN DE ACTIVOS. | ANÁLISIS Y TRATAMIENTO DE RIESGOS | AUDITORÍA E INCIDENCIAS DE SEGURIDAD. | CUADRO DE MANDO DE SEGURIDAD

Informe de activos

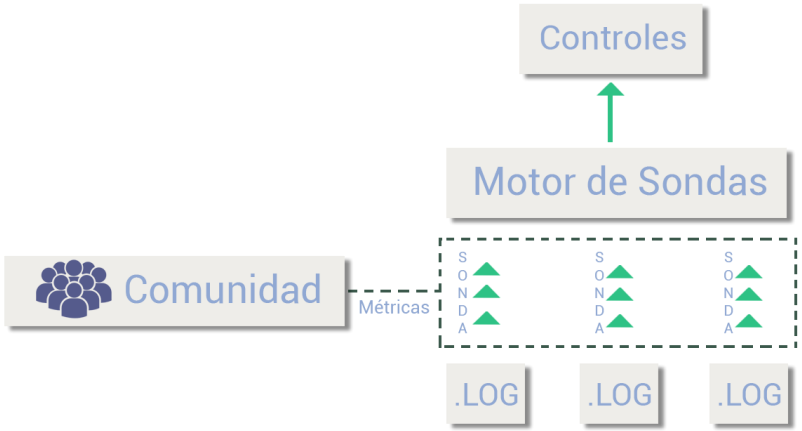
Informe de auditoría

MARISMA

- MARISMA por lo tanto, es una metodología soportada por una herramienta (eMARISMA), que permite la realización de Análisis de Riesgo: **usando Patrones Reutilizables de Conocimiento, de Bajo Coste, Dinámicos, y Homogéneos.**
- Pero que tiene el objetivo de permitir la creación de una **Mente Colmena** que aprende de los riesgos mediante técnicas de **Machine Learning**, permitiendo a las compañías proteger mejor sus activos críticos.


PATRONES
Dominios
Tipo Activo
Dimensiones
Tipo Amenaza
Objetivos
Objetivos
Amenazas
Amenazas
Controles
Tipo Activo
Amenaza
Dimensión
Checklist
Activos
Machine Learning

SONDAS + MÉTRICAS



JERARQUÍA DE ACTIVOS

Conclusiones del Apartado

1. Las Infraestructuras Criticas son un paso en la dirección correcta, pero requieren todavía de importantes avances que deben venir de Instituciones Publicas y Universidades, apoyadas por las Empresas.
2. Ahora mismo existen importantes proyectos como MARISMA, que buscan alinear Instituciones públicas y privadas, así como grandes y pequeñas compañías, con el objetivo de generar sinergias a la hora de crear las estructuras de defensa contra las amenazas, utilizando para ello nuevos conceptos avanzados de ciberseguridad.

Conclusiones Finales

Conclusiones Finales

1. Las Infraestructuras Criticas se presentan como un **paradigma critico** a la hora de poder mantener la **estabilidad de las naciones**.
2. Pero también es un campo muy joven, en el que **queda mucha investigación práctica por desarrollar**.
3. Las Infraestructuras Criticas no se pueden ver como algo aislado, sino que **deben verse con una visión global y mundial**.
4. La verdadera defensa contra las amenazas pasa por alinear la seguridad de todas las compañías creando un **muro único de seguridad global.**

Conclusiones Finales

MARISMA nace con ese objetivo

Ayudar a crear soluciones, mediante la **creación de una comunidad** que permita unificar los esfuerzos de seguridad global, **centralizando el conocimiento** y utilizándolo para **ser más eficiente** a la hora de **combatir las amenazas**.

UCLM
UNIVERSIDAD DE CASTILLA-LA MANCHA

GSyA
Grupo de Investigación en Seguridad y Auditoría

SICAMAN

www.sicaman-nt.com
www.emarisma.com

CASTILLA LAMAN CHA

¿Preguntas?

Dr. Luis Enrique Sánchez Crespo
luisenrique@sanchezcrespo.org