MNEMO
NEGOCIO
CIBERSEGURIDAD
CONECTIVIDAD

MNEMO

Conocer y aplicar la Ciberseguridad

LA SEGURIDAD CONECTADA

Alfonso Juan Minaya
(BDM)
a.minayagallego@Mnemo.com

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

¿Quíenes Somos?

Somos una compañía multinacional española, Con SOC CERT en Colombia, México y España. Nuestra vocación son la Tecnología y la Seguridad, ambas estrechamente ligadas por la globalización y digitalización del mundo en que vivimos..

El Equipo profesional de MNEMO está constituido por más de 700 personas, constituyendo un grupo muy sólido técnicamente, con muchos años de experiencia en el mercado y que incorpora desde su I+D nuevo talento para Innovar en este mundo en constante evolución.

Contamos con 3 SOC Cert, somos miembros de CSIRT.es y miembros del grupo FIRST

MN-MO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

¿Cómo nos organizamos?

Mnemo tiene una clara idea de que a día de hoy la seguridad física y la lógica tienen que ir de la mano, nuestros clientes reciben un sistema para evaluar su seguridad, según la criticidad de sus activos y unos protocolos de actuación cuando dichos activos ven "mermados su nivel de seguridad".

Nuestra apuesta es la convergencia.

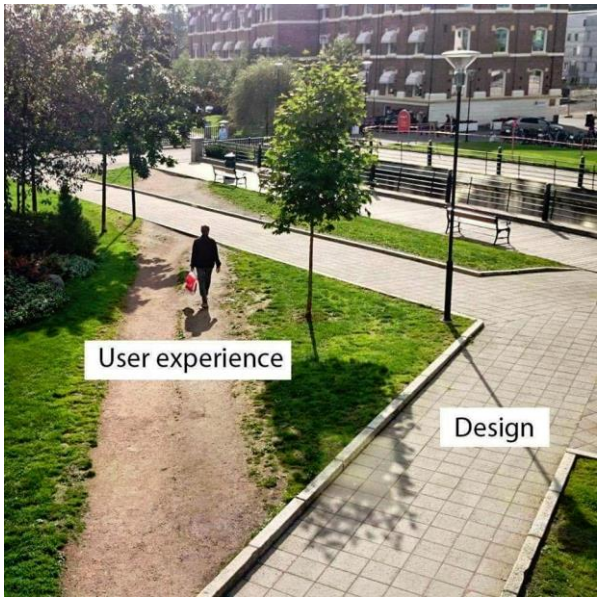
Somos Expertos en la integración

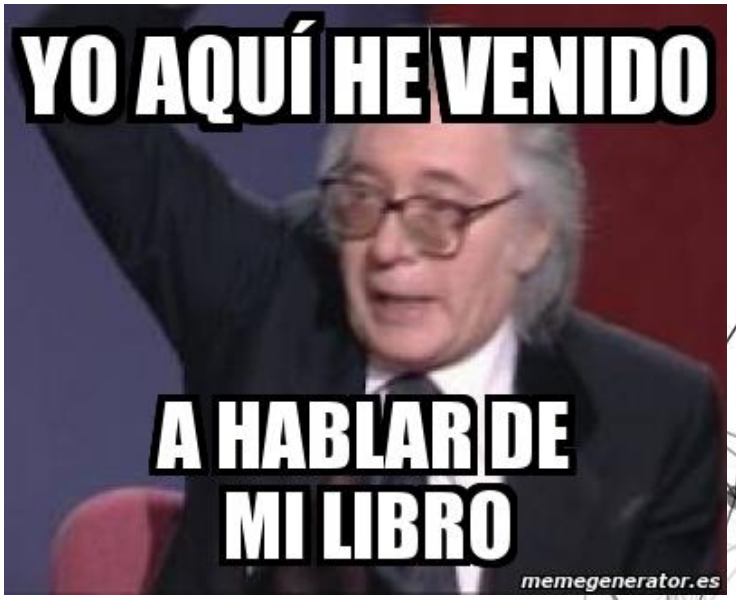
MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Lo primero escuchar

Mnemo no quiere ser un proveedor sino un aliado, el apoyo en la búsqueda de soluciones.

Para nosotros es tan importante la Ingeniería como la experiencia del usuario





Concienciar

Debemos concienciar a los usuarios, a los directivos que la protección de los activos, de la información es un ejercicio diario de TODOS los empleados de la empresa.

Pero debemos hablar en un idioma que nos entiendan

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Los malos

Es uno de los “negocios” más lucrativos del mundo.

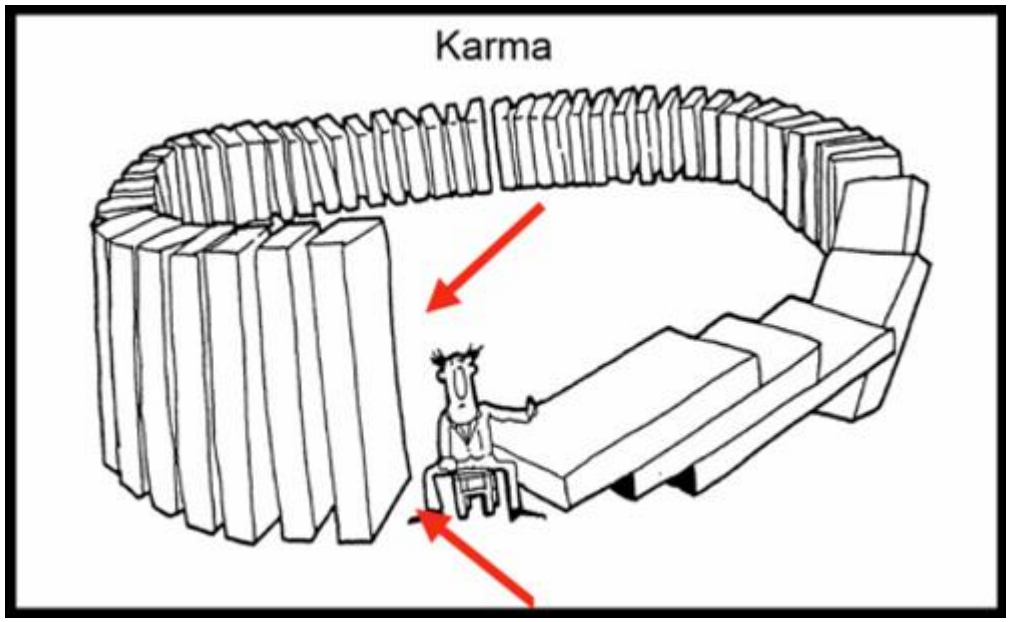
Ya no se busca a la gran empresa sino se busca a la empresa con posibilidades de ser más vulnerable (IA).

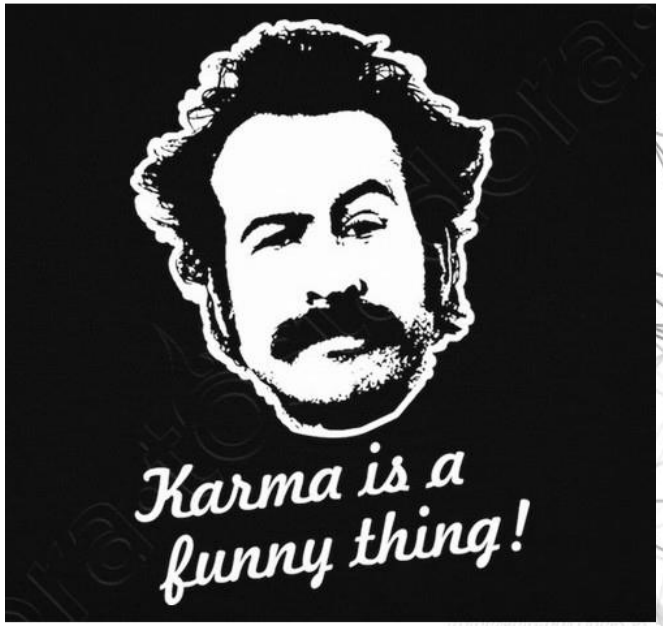
Todos estamos expuestos, no por ser grandes o pequeños, sino por estar conectados

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Un ejemplo WannaCrypt

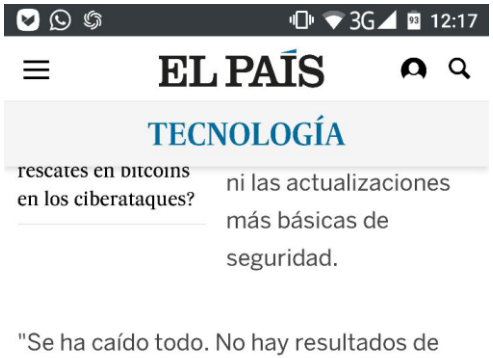
Según informó The New York Times, **la vulnerabilidad EternalBlue, utilizada por los autores del ataque para propagar un ransomware llamado WannaCry, fue filtrada en abril por el grupo de hackers Shadow Brokers**, que ha estado aireando en Internet herramientas supuestamente empleadas por la Agencia Nacional de Seguridad (NSA).
Microsoft, que describió esta vulnerabilidad en el boletín de seguridad MS17-010, dijo que sus ingenieros añadieron este viernes "detección y protección contra el nuevo software malicioso, conocido como Ransom:Win32.WannaCrypt".



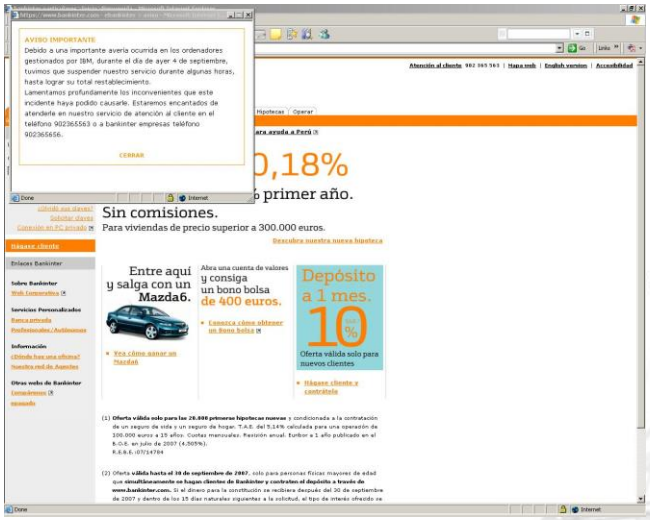


MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Y llego el Caos

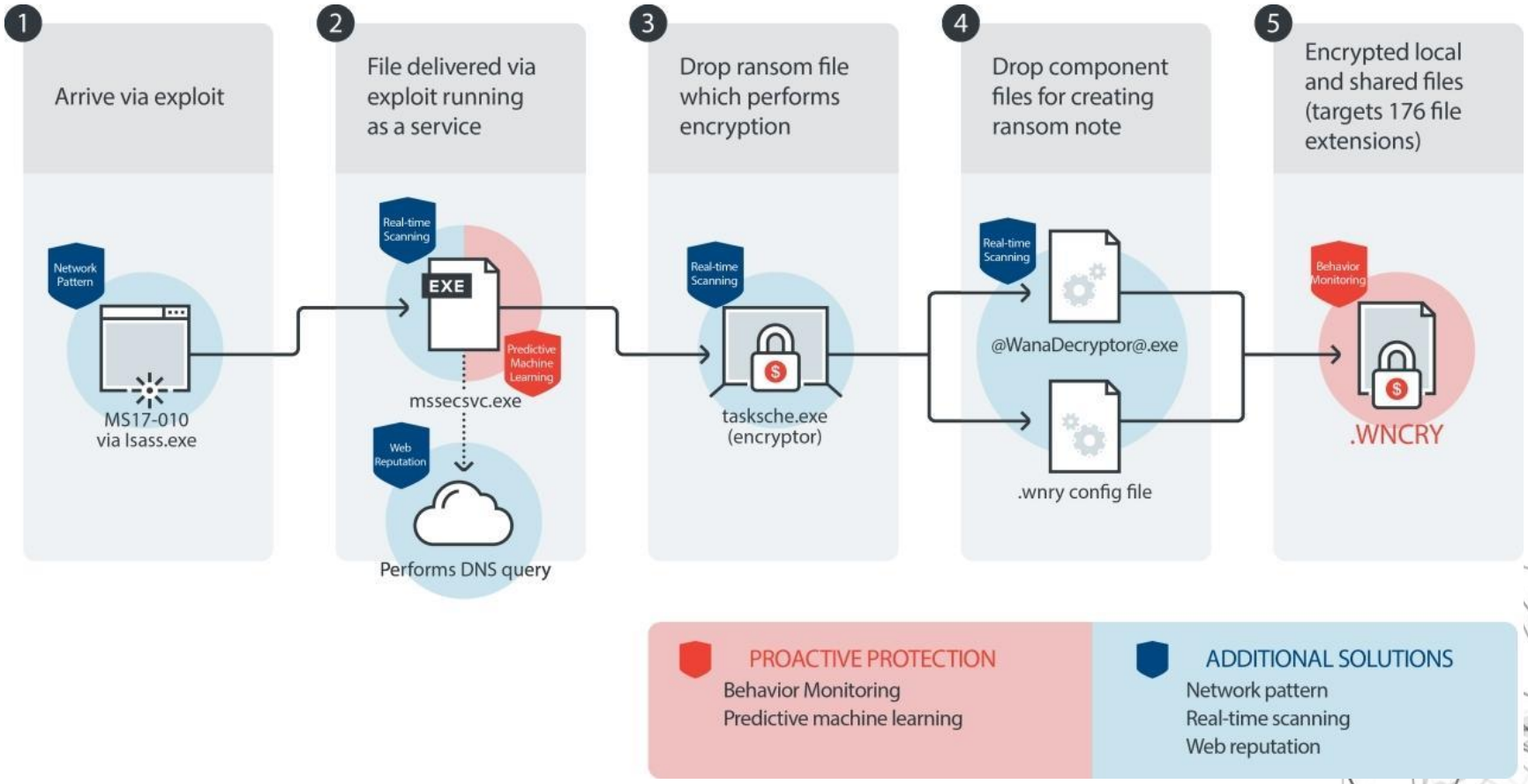


"Se ha caído todo. No hay resultados de análisis de sangre, ni radiografías, ni sangre de un grupo sanguíneo específico", escribió este viernes un doctor de uno de los hospitales afectados en Londres. "No podemos realizar ningún tratamiento que no sea cuestión de vida o muerte. Va a morir gente por esto".



MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Qué hace el "bichito"



MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Qué ocurrió en las empresas

la ciberseguridad no es un gasto si no una inversión

Un dominio de 10 dólares para contener un ciberataque "sin precedentes"

Dos investigadores dedujeron que la solución al malware que ha afectado a 99 países pasaba por dirigir el virus a un dominio específico que compraron por 10,69 dólares.

Telefónica

LA INTRANET GLOBAL

13 / 03 / 2017

ELEGIMOS TODO_

URGENTE: APAGA TU ORDENADOR YA

El equipo de Seguridad ha detectado el ingreso a la red de Telefónica de un malware que afecta tus datos y ficheros. Por favor avisa a todos tus compañeros de esta situación.

Apaga el ordenador ya y no vuelvas a encenderlo hasta nuevo aviso(*).

Te enviaremos un correo que podrás leer a través de tu móvil cuando la situación ya esté normalizada. Además, el martes informaremos en las entradas de los edificios sobre el acceso a la red.

Ante cualquier duda contacta con la Mesa de Ayuda (29000)

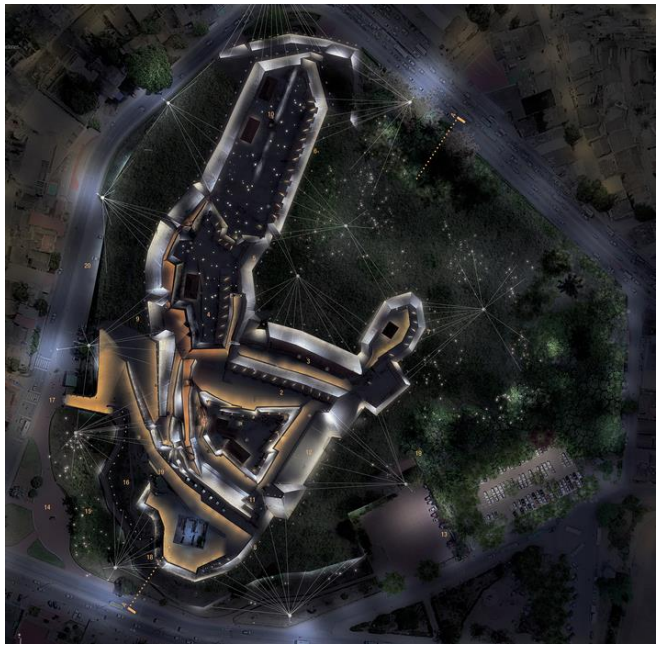
(*) Desconecta el móvil de la red WiFi pero no hace falta que lo apagues

Dirección de Seguridad

En compañías como Vodafone, Iberdrola o Gas Natural han pedido a sus empleados que apaguen el ordenador

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Nuestra empresa, un castillo, una fortaleza



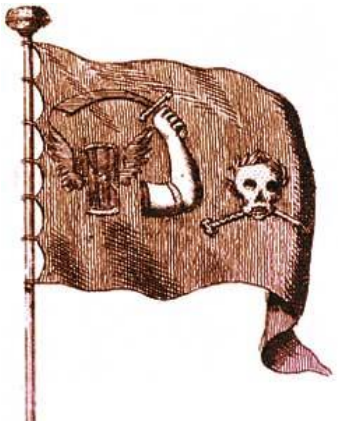
Pensamos que nuestra empresa es una fortaleza, un castillo capaz de aguantar las mayores embestidas, pero ...

...puede compararse a un hombre insensato, que edificó su casa sobre arena. Cayeron las lluvias, se precipitaron los torrentes, soplaron los vientos y sacudieron la casa: ésta se derrumbó, y su ruina fue grande"
(Mateo 7, 24-27)

Castillo de San Felipe – Cartagena de Indias- Colombia

Nuestra misión .- Defenderla

"War of Jenkins' Ear",



La batalla de Cartagena de Indias, del 13 de marzo al 20 de mayo de 1741.
Ingleses
186 buques, con 27 600 hombres, armada con 2000 cañones.
Españoles
Las fortificaciones de la ciudad . 3600 hombres y de una flota de seis buques: el *Galicia*, el *San Carlos*, el *San Felipe*, el *África*, el *Dragón* y el *Conquistador*.

Bajas Españolas
200 muertos , 6 barcos 5 fuerte y 3 baterías de tierra
Bajas Inglesas
18000 muertos, 1500 cañones y 50 barcos.

Consecuencias – Se sigue hablando castellano en el caribe
Impuesto del te en Inglaterra
Guerra de independencia(USA)

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Cómo lo Hacemos

Intelligent SOC
Seguridad Conectada

Emulando a nuestro sistema Inmune.

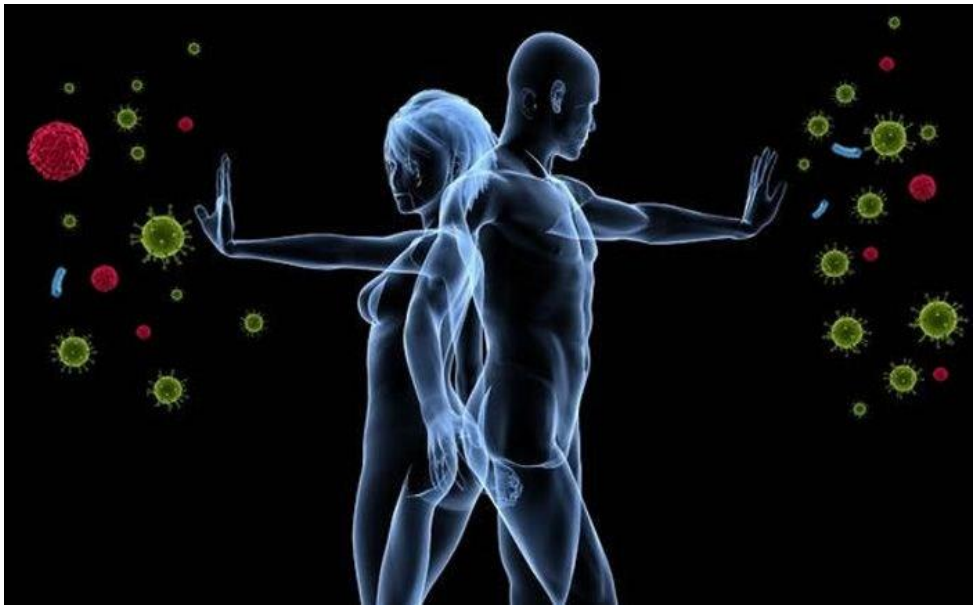
Nuestros Pilares

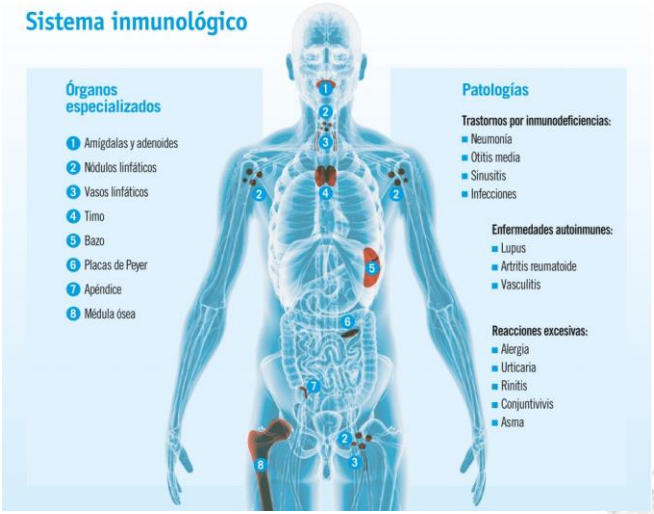
1. ADAPTATIVA
Emular un sistema inmunitario eficaz que sea capaz de adaptarse para poder reconocer y hacer frente a la amenaza.

2. EVOLUTIVA
Evolucionar con madurez para hacer frente al mayor reto que plantea hoy cualquier amenaza: Su constante Evolución

3. INTELIGENTE
Aplicar métodos basados en Inteligencia para apoyar la toma de decisiones de manera preventiva, y reactiva una vez ocurra un incidente.

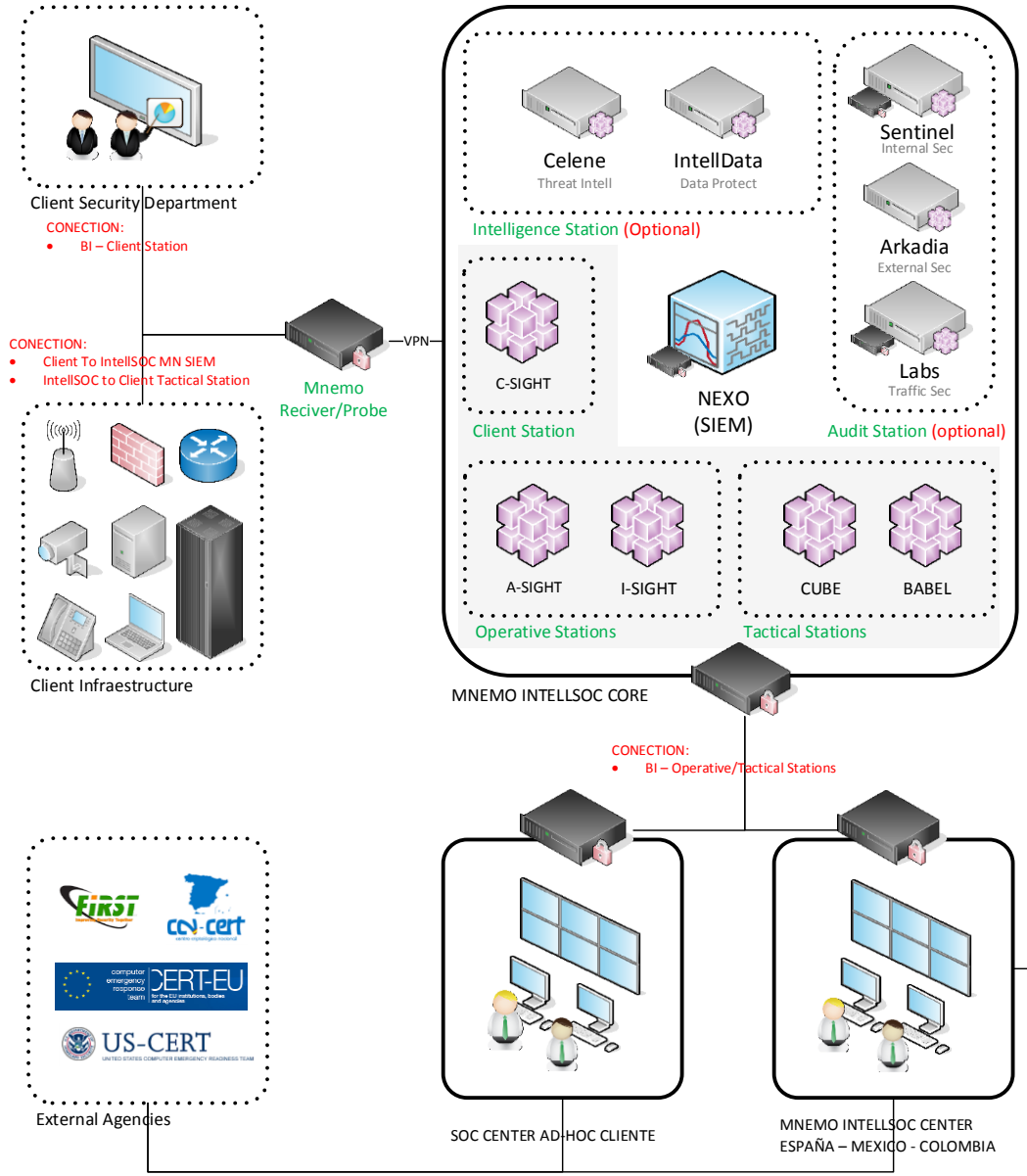
4. ESTRATÉGICA
Conocer en qué nivel de riesgo se encuentra una organización y qué medidas se deben tomar es un proceso clave que debería poder llevarse a cabo de forma sencilla.





MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Cómo lo Hacemos



Módulos Core del Servicio IntellSOC

Módulos opcionales para ampliación de servicio IntellSOC

Plataforma de conexión y funcionalidad

Servicios Mnemo Intelligence Security Center

Seguridad Gestionada
Servicios de SOC externo, Servicio gestión seguridad, Mantenimiento Seguridad

Auditorias Seguridad
Servicios de Auditoria Estática, Experta, Evolutiva y Continua

Mnemo Ingenieria
BBDD de entidades relacionadas con actores y patrones

Mnemo CION
Soluciones de inteligencia corporativa
Soluciones de inteligencia FCSE

Mnemo LABS
Análisis Experto de tráfico y malware, análisis forense y dispositivos elect.

Mnemo Director
Adaptación legal y normativa bajo metodología y herramienta INTEGRA

Mnemo Vital
SOC, ingenieria, y tecnología para II.CC y seguridad industrial

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

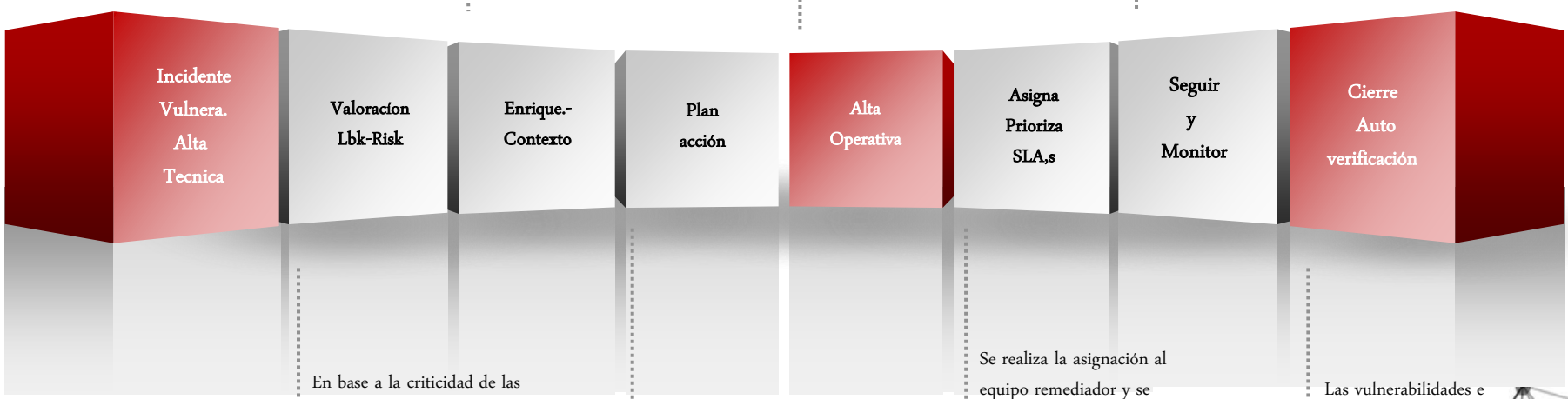
Cómo lo Hacemos

Descubrimiento por alerta temprana, persistente o experto, gestiónado con los sistemas automátizados y equipos expertos

La vulnerabilidad se enriquece añadiendo metadatos de estructura y negocio para valoración estratégica

Se registra el incidente o vulnerabilidad enriquecida, para su gestión y tratamiento en la estructura.

Desde el sistema se puede analizar la repercusión de la misma, hacer un seguimiento del proceso de remediación y monitorizar su resolucón.



En base a la criticidad de las áreas, de los activos y las características de la vulnerabilidad se recataloga el riesgo inicial a riesgo cliente

Se establece un plan de acción inmediato con remediación, virtual patching y acción crítica

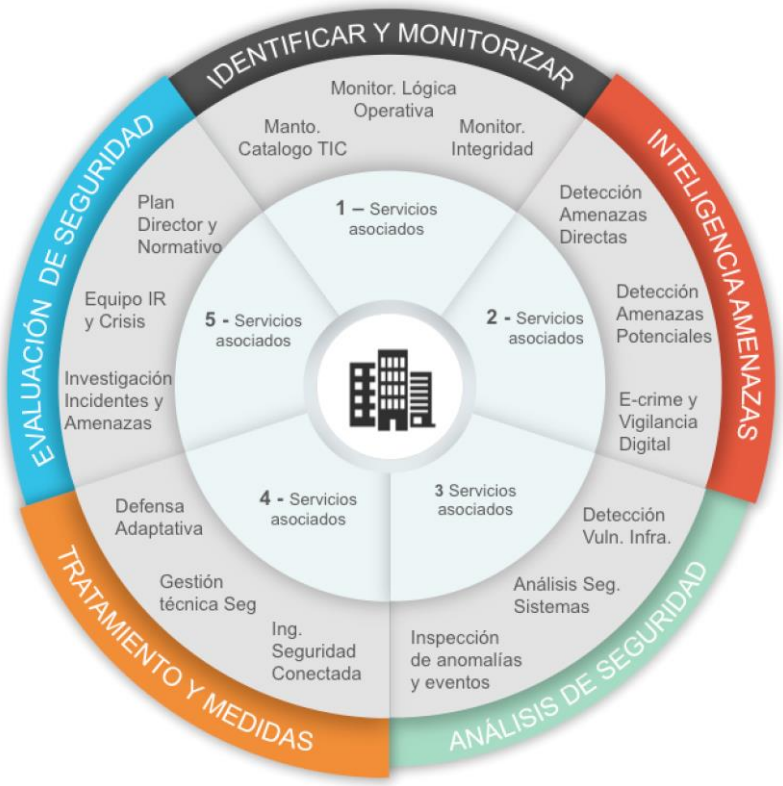
Se realiza la asignación al equipo remediador y se establecen lo SLA,s, el sistema establece los sistemas de aviso y alerta

Las vulnerabilidades e incidentes se cierran y autoverifican su correcta solución .

"Se trata de ser capaz de enfocar nuestros esfuerzos en las cosas correctas, por las razones correctas, en el menor tiempo posible"

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

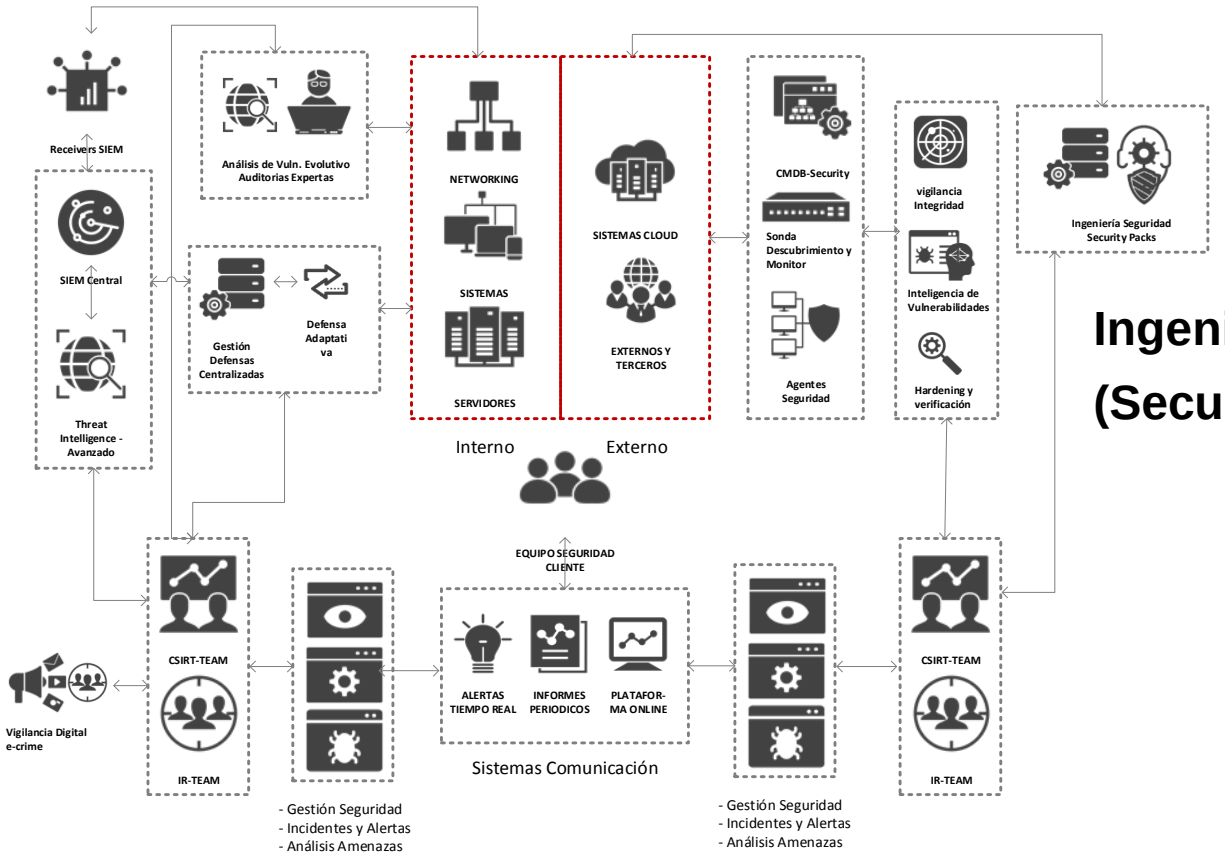
Cómo lo Hacemos



- Metodología diseñada para conocer el estado de la Seguridad de cualquier organización, con independencia del tamaño y actividad.
- Segmentada en 5 bloques funcionales.
- Hoja de ruta personalizada y adaptable a la estrategia de ciberseguridad de cada organización.
- Servicio integral de Ciberseguridad.

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Cómo lo Hacemos



Ingeniería Seguridad (Security Packs)

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Los Grandes problemas de la Ciberseguridad en 2018

Ransomware: el "malware" de mayor crecimiento

Infecciones de malware sin archivo
2016 se intensificaron los ciberataques con este método, pero variando su técnica a la infección de los ordenadores sin que medie la descarga de algún archivo.

Ataque de denegación de servicio en servidores y sistemas web globales

Tráfico malicioso: protocolos cifrados como señuelo.
2016 creció el tráfico de este protocolo cifrado que encubría "malware" y otras actividades maliciosas multiplicándose por cinco.

Malvertising: "malware" disfrazado de publicidad.

Phishing y Spearphishing: estafas más realistas y verosímiles
buscan engañar a un miembro de una organización para acceder a sus sistemas e información de forma fraudulenta.

Fraude en el mundo real para acceder a información digital.

Ciberdelincuencia con IA

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Los Grandes retos de la Ciberseguridad en 2018

RETO 1: RGPD y el precio de la privacidad

La protección de datos es una preocupación fundamental en un mundo cada vez más digital y el 25 de mayo de 2018 se produjo un punto de inflexión para la protección de datos en Europa con la entrada en vigor del nuevo Reglamento General de Protección de Datos de la UE (GDPR, por sus siglas en inglés).

El incumplimiento puede dar lugar a multas de hasta el 4% de la facturación global, una cantidad que puede ser letal para muchas empresas, especialmente las PYMES.

RETO 2: IoT y la convergencia de seguridad, ciberseguridad y privacidad de datos

En 2016, Mirai demostró que los dispositivos de Internet de las cosas (IoT) pueden ser armados efectivamente como botnets, la rapidez con la que se desarrollan los productos, así como el tiempo de puesta en mercado y la falta de mantenimiento por parte de los fabricantes (y usuarios) hacen que **los dispositivos de IoT estén muy expuestos a la explotación de vulnerabilidades críticas.**

RETO 3: la industria 4.0 emerge como primer objetivo para cibeataques

Industria 4.0 ya está transformando la industria y la infraestructura a nivel global, prometiendo una mayor eficiencia, productividad y seguridad. Hoy en día, para mantener la competitividad es necesario digitalizar gran parte de los procesos de producción, lo hace que todos los componentes de estas cadenas estén expuestos a ataques cibernéticos debido a sus vulnerabilidades.

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

Los Grandes retos de la Ciberseguridad en 2018

RETO 4: Centrarse en la detección y respuesta temprana a amenazas

os recientes, y mediáticos, ciberataques a organizaciones de perfil alto, demuestran que los controles preventivos, por sí solos, no son suficientes.

Las empresas se enfrentan a un escenario donde se ha incrementado el volumen de datos de registro de seguridad, no se está haciendo un uso adecuado de la inteligencia sobre amenazas, hay incapacidad para monitorizar los dispositivos IoT.
Esto está provocando que, en la actualidad, las organizaciones tardan, de media, más de 191 días en detectar una violación de seguridad, y que supone un alto coste para las empresas.
Por eso es necesario centrarse más en acortar el tiempo que lleva detectar y responder a un ataque, que permita minimizar daños, y no tanto en incrementar las medidas defensivas.

RETO 5: Aumento del uso de la IA para ciberataques y defensa cibernética

Hay un volumen creciente de ciberataques cada vez más sofisticados y persistentes. El malware se está volviendo más capaz de adaptarse de forma 'inteligente' y evadir las medidas tradicionales de detección y erradicación.
El volumen de datos de seguridad excede ahora con creces nuestra capacidad natural para usarlo de manera efectiva, lo que lleva a la necesidad de empezar a usar herramientas de IA aplicadas a la ciberseguridad.

MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

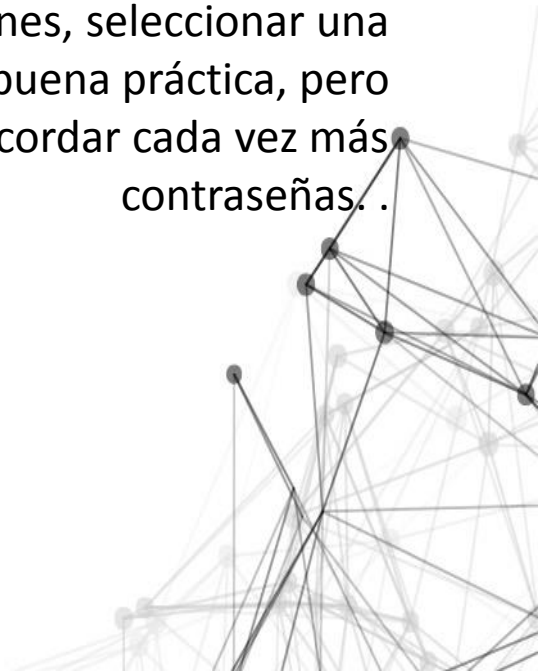
Los Grandes retos de la Ciberseguridad en 2018

RETO 6: Certificaciones para inyectar confianza en la ciberseguridad

Tanto en las empresas de servicios, la certificación continua de los técnicos, las certificaciones internacionales de servicios (SOC CERT) etc.

RETO 7: Autenticación biométrica reemplaza las contraseñas

Nuestras vidas digitales se rigen por una compleja red de aplicaciones en línea, cada una de las cuales requiere un nombre de usuario y una contraseña para controlar el acceso. Proteger los datos que se encuentran detrás de estas aplicaciones, seleccionar una contraseña oscura y compleja, y cambiarla a menudo, es una buena práctica, pero también resulta en una gran complejidad para el usuario que debe recordar cada vez más contraseñas. .



MNEMO NEGOCIO CIBERSEGURIDAD CONECTIVIDAD

No nos olvides, nosotros no lo haremos

Cuando llamas al servicio tecnico, no hablaras con una maquina, no tendrás que explicar tu red, si somos aliados debemos conocerte .

Mnemo, diseñados para acompañar a sus clientes en el camino hacia el éxito