Tu socio tecnológico

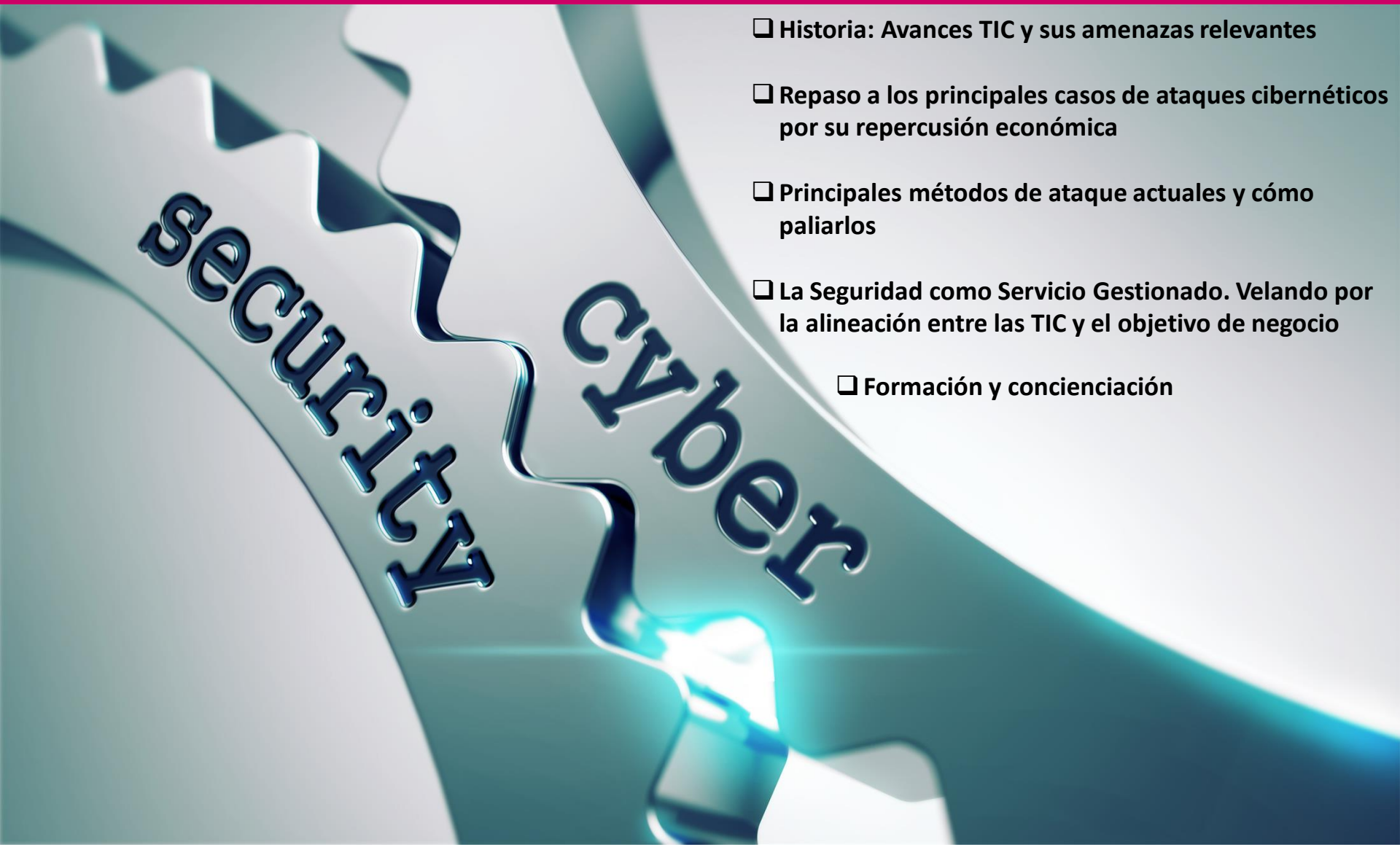
nunsys®

COMUNICACIONES · SISTEMAS · SOFTWARE · MARKETING · FORMACIÓN

Concienciación de riesgos de Ciberseguridad Informática

economistas
Colegio de Valencia

CONCIENCIACIÓN DE RIESGOS DE CIBERSEGURIDAD INFORMÁTICA



- Historia: Avances TIC y sus amenazas relevantes
- Repaso a los principales casos de ataques cibernéticos por su repercusión económica
- Principales métodos de ataque actuales y cómo paliarlos
- La Seguridad como Servicio Gestionado. Velando por la alineación entre las TIC y el objetivo de negocio
- Formación y concienciación

PREÁMBULO

PUNTOS DESTACABLES

¿Qué es la ciberseguridad?

Seguridad de la información <> Ciberseguridad

Ciberseguridad – Protección de la información digital y de los activos en los que se hospeda, procesa y transfiere a través de sistemas interconectados

Seguridad de la información es la ciencia que se encarga de mitigar los riesgos, que amenazan a la información, hasta conseguir un umbral aceptable por el propietario/responsable de la misma y de disponer de un control continuo para conseguir mantener ese umbral

CIBERSEGURIDAD
CIBERAMENAZAS
CIBERSPACIO
CIBERGUERRA
CIBERDELITOS
CIBERACTIVISTAS
CIBERTERRORISMO

ATAQUES CIBERNÉTICOS

ATAQUES INFORMÁTICOS

¿Objetivos de la ciberseguridad?

Velar por:

- Disponibilidad
- Confidencialidad
- Integridad
- Autenticidad
- Trazabilidad

Seguridad 100% – No existe => Capas coordinadas y bien gestionadas

El eslabón más débil -> El humano

A MI NO ME VA A PASAR. Y SI ME PASA, EL IMPACTO SERÁ PEQUEÑO

- ***Dispongo de seguridad perimetral***
- ***Dispongo de antivirus***
- ***No soy una empresa objetivo de ataque***
- ***Mis empleados no acceden a páginas comprometidas***
- **…**

Daños:

Pérdida de información – Robo / Secuestro / Destrucción
Pérdida de negocio – Corte en la producción / servicio
Dedicación de Recursos Humanos – Recuperación / Alternativas
Reputación - ¡Trabajan con mis datos! / ¿Aseguran el servicio?
Responsabilidad ante terceros – Incumplimientos legales - Sanciones
Rescate - ?????

HACKER <> CRACKER

HACKER – Especialista informático capaz de romper las barreras de seguridad de una infraestructura y/o sistema informático a fin de velar por la seguridad

CRACKER – Es aquél especialista informático que es capaz de romper las barreras de seguridad para realizar acciones ilícitas.

ORGANISMOS OFICIALES DE DEFENSA

CCN-CERT, Equipo de respuesta del Centro Criptológico Nacional dependiente del Centro Nacional de Inteligencia, con un ámbito competencial en el Sector Público local, autonómico y nacional.

INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, con un ámbito competencial en los ciudadanos, empresas, operadores de servicios esenciales e instituciones afiliadas a RedIRIS, la red académica y de investigación española. INCIBE-CERT será operado conjuntamente por el INCIBE y el CNPIC en todo lo que se refiera a la gestión de incidentes que afecten a los operadores críticos.

Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC)
Con un ámbito competencial en las infraestructuras críticas y operadores críticos, cuyas capacidades de respuesta técnica se materializan a través de los CSIRT de referencia

ESPDEF-CERT del Mando Conjunto de Ciberdefensa
Con un ámbito competencial en las redes y los sistemas de información y telecomunicaciones de las Fuerzas Armadas, así como aquellas otras redes y sistemas que específicamente se le encomienden y que afecten a la Defensa Nacional

Equipos, Foros y Roles

CERT *Computer Emergency Response Team*
Centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. De cuño **EEUU**

CSIRT *Computer Security Incident Response Team*
Es como se llama a los CERT en **Europa**

FIRST *Forum of Incident Response and Security Teams*.
Es la principal organización y líder mundial reconocido en respuesta a incidentes. FIRST permite a los equipos de respuesta a incidentes responder de manera más efectiva a los incidentes de seguridad tanto reactivos como proactivos.

FIRST reúne una variedad de equipos de respuesta a incidentes de seguridad informática de organizaciones gubernamentales, comerciales y educativas. FIRST tiene como objetivo fomentar la cooperación y la coordinación en la prevención de incidentes, estimular una reacción rápida a los incidentes y promover el intercambio de información entre los miembros y la comunidad en general.

Más de 500 miembros distribuidos en África, América, Asia, Europa y Oceanía.

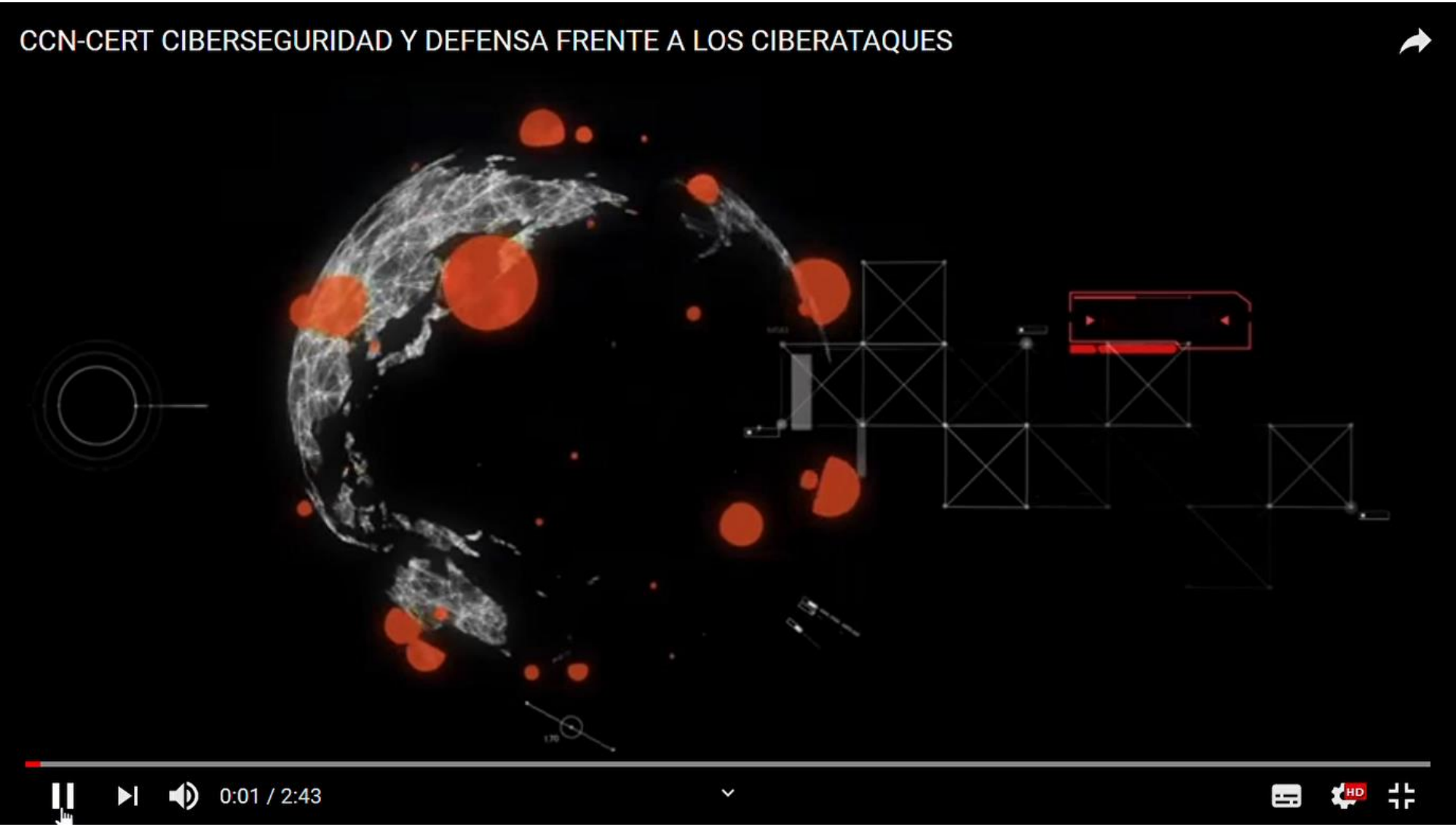
Equipos, Foros y Roles

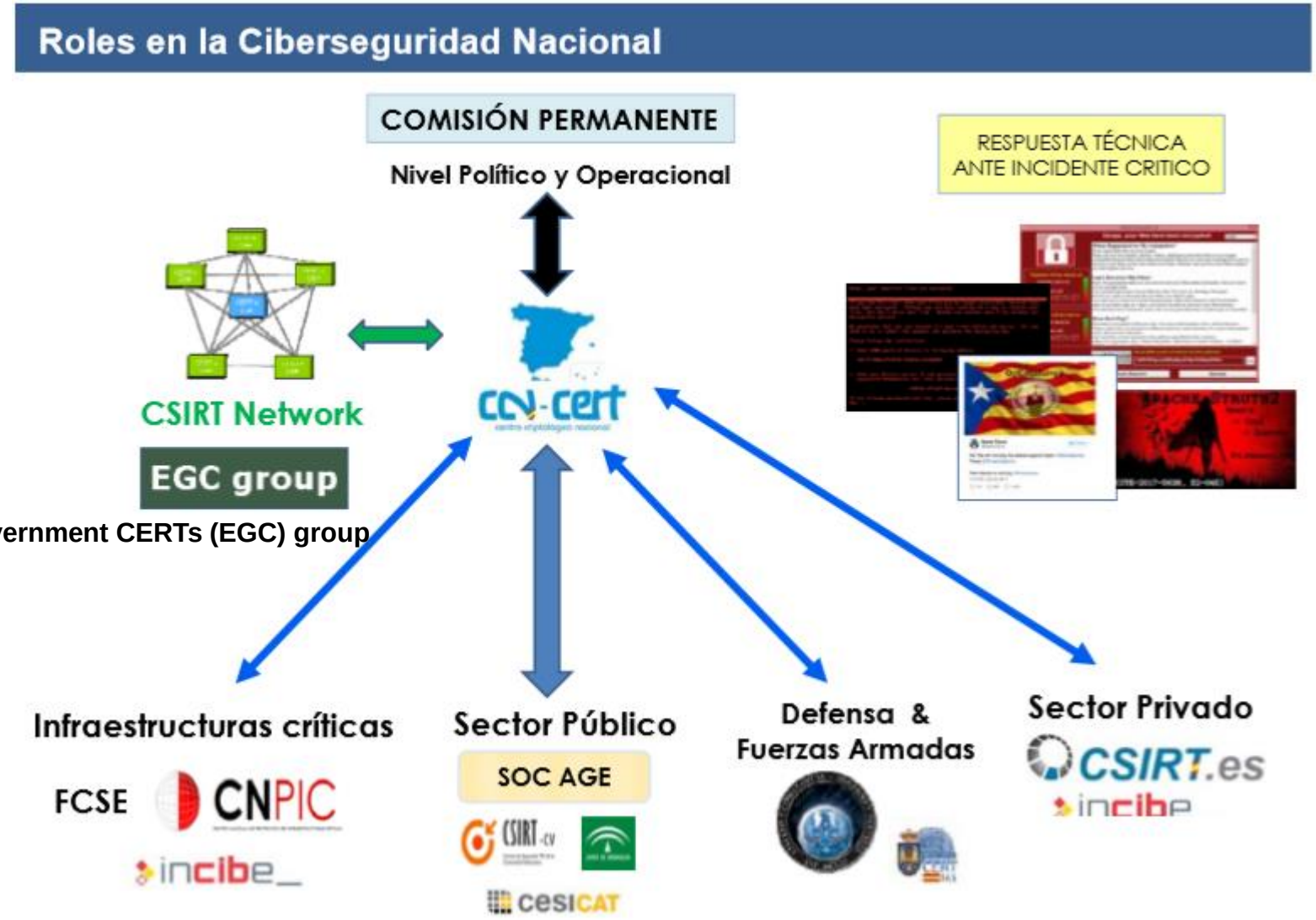
TF-CSIRT *Task Force on Computer Security Incident Response Team*
Provee un foro Europeo donde los miembros de la comunidad **CSIRT** pueden intercambiar experiencias y conocimientos en un ambiente de confianza con el fin de mejorar la cooperación y la coordinación.
Mantiene un sistema de registro y acreditación de los CSIRT, así como la certificación de los estándares de servicio. El grupo de trabajo también desarrolla y ofrece servicios para los CSIRT, promueve el uso de las normas y procedimientos para el manejo de incidentes de seguridad comunes, y coordina las iniciativas conjuntas en su caso. Esto incluye la formación del personal del CSIRT, y ayudar en la creación y desarrollo de nuevos CSIRT.

DPO Data Protection Officer

PSO Plan Seguridad del Operador
PPE Plan de Protección Específico

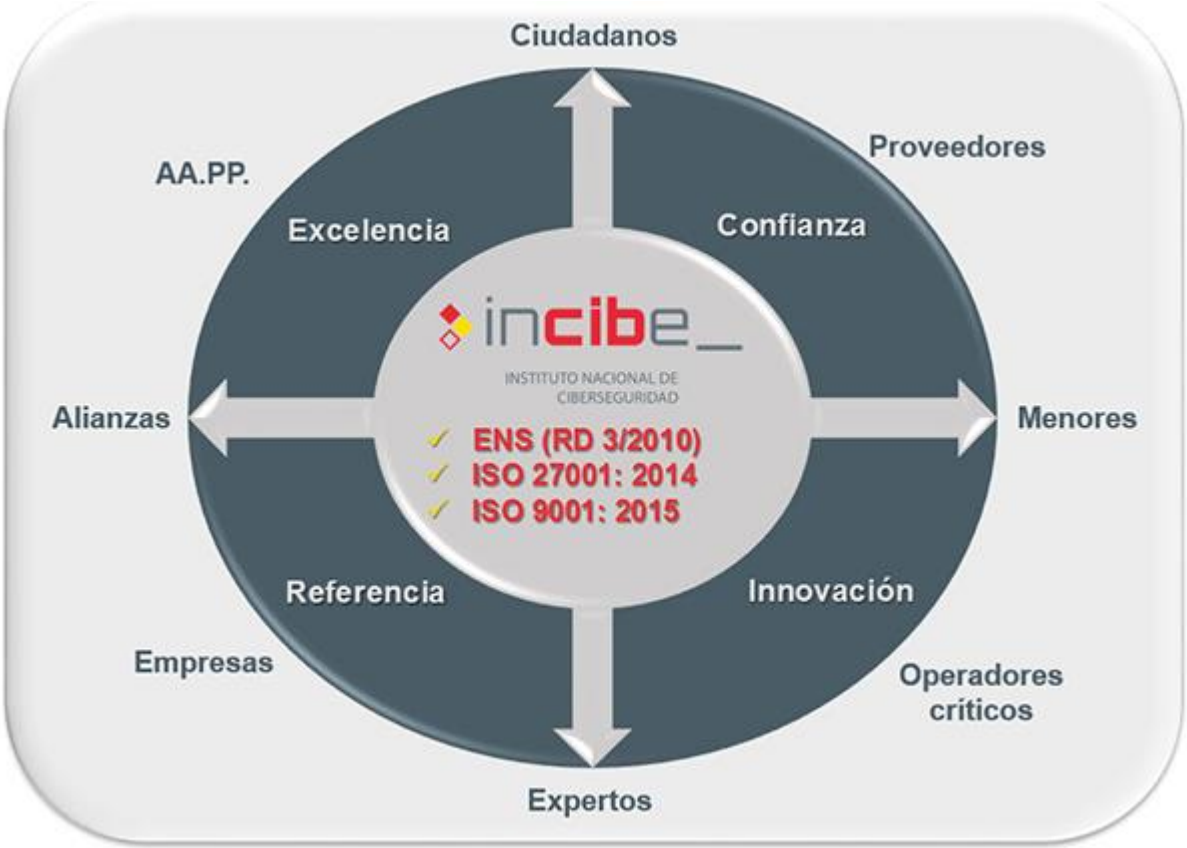
PUNTOS DESTACABLES




Roles en la Ciberseguridad Nacional
COMISIÓN PERMANENTE
Nivel Político y Operacional
RESPUESTA TÉCNICA
ANTE INCIDENTE CRITICO
CSIRT Network
EGC group
European Government CERTs (EGC) group
Infraestructuras críticas
FCSE
CNPIC
incibe_
Sector Público
SOC AGE
CSIRT.cv
cesicat
Defensa &
Fuerzas Armadas
Sector Privado
CSIRT.es
incibe

PUNTOS DESTACABLES

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD



DIRECTIVAS, NORMATIVAS Y ESTÁNDARES

Directiva NIS, (Network and Information System)
"Directiva del Parlamento Europeo y del Consejo relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información de la Unión"
Entró en vigor el 9 de agosto del 2018

Busca mejorar la fragmentación existente en los Estados y homogeneizar los distintos planteamientos, estableciendo requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los **operadores de servicios esenciales** y los **proveedores de servicios digitales**.

RGPD (Reglamento General de Protección de Datos)
El Reglamento General de Protección de Datos (Reglamento de la UE 2016/679) es el nuevo marco jurídico de la UE que rige el uso de los datos personales. Este texto deroga la anterior Directiva 95/46/CE de protección de datos y sustituye a las leyes de protección de datos nacionales existente (En España, la Ley 15/1999 de Protección de Datos). El texto es aplicable en todos los mercados de la Unión Europea desde el 25 de mayo de 2018.

DIRECTIVAS, NORMATIVAS Y ESTÁNDARES

LOPDGDD Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales.
03/2018 de 5 de diciembre
Adapta al contexto español el RGPD europeo.
Además, restringe y especifica de manera más clara las infracciones y multas derivadas de la misma.

ISO27001
Es un estándar para la seguridad de la información aprobado y publicado como estándar internacional en octubre de 2005 por *International Organization for Standardization* (**ISO**) y por la comisión *International Electrotechnical Commission* (**CEI**).
Establece el marco de trabajo para definir un **SGSI**, centrándose en la visión de la gestión de la seguridad como un proceso continuo en el tiempo.

SGSI Sistema de gestión de la seguridad de la información.
Consiste en normativa, procedimientos y guías, junto con sus recursos y actividades asociadas, usados de forma coordinada por una organización que busca proteger sus activos de información.

Un SGSI es una aproximación sistemática para establecer, implantar, operar, supervisar, revisar, mantener y mejorar la ***seguridad*** de la información de una organización a fin de alcanzar sus ***objetivos de negocio***. Se basa en el análisis de riesgos y la asunción controlada de un cierto nivel de riesgo con el objetivo de tratar y gestionar efectivamente los riesgos

DIRECTIVAS, NORMATIVAS Y ESTÁNDARES

ENS Esquema Nacional de Seguridad

1. La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

Aplica a:

- A la Administración General del Estado, Administraciones de las Comunidades Autónomas y las Entidades que integran la Administración Local, así como las entidades de derecho público vinculadas o dependientes de las mismas.
- A los ciudadanos en sus relaciones con las Administraciones Públicas.
- A las relaciones entre las distintas Administraciones Públicas.

Ley PIC – Protección de Infraestructuras Críticas

Los dos grandes objetivos de esta norma son:

- Catalogar el conjunto de infraestructuras que prestan servicios esenciales a nuestra sociedad.
- Diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones

Tu socio tecnológico

nunsys®

COMUNICACIONES · SISTEMAS · SOFTWARE · MARKETING · FORMACIÓN

economistas
Colegio de Valencia

Historia

Avances TIC y sus amenazas relevantes

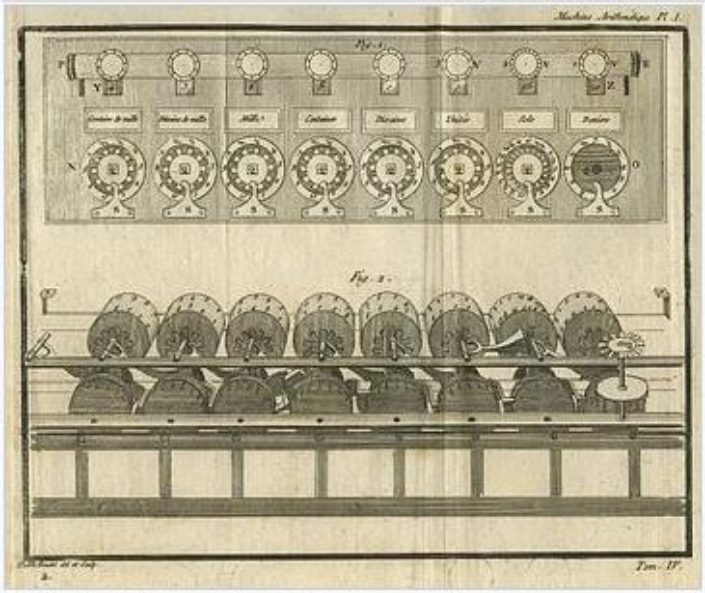
UN POCO DE HISTORIA - Evolución de las TIC

Entre el **500 y 300** A.C.
El **ábaco**. Se considera la primera máquina capaz de realizar cálculos.

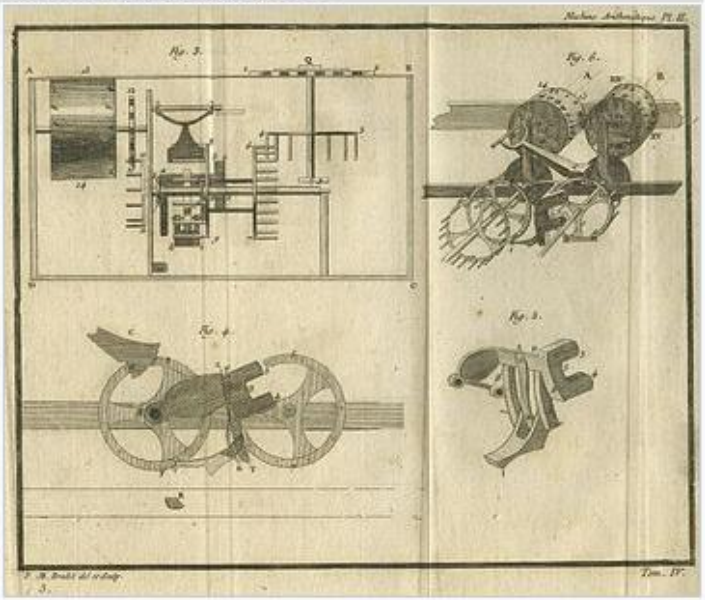
1642.
La **Pascalina** (máquina aritmética / rueda pascalina)
Blaise Pascal
Sumas / Restas

Mecanismo de ruedas dentadas enlazadas entre sí

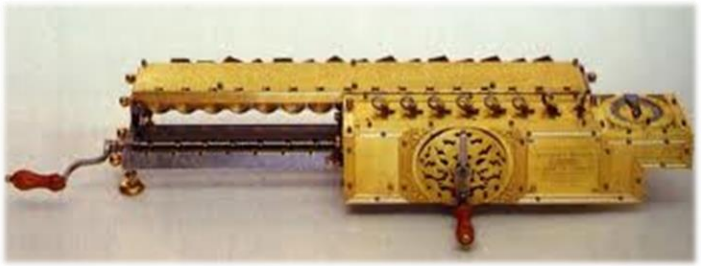
Obras de Pascal en 5 volúmenes, La Haya, 1779



Cubierta de la pascalina y todo su mecanismo



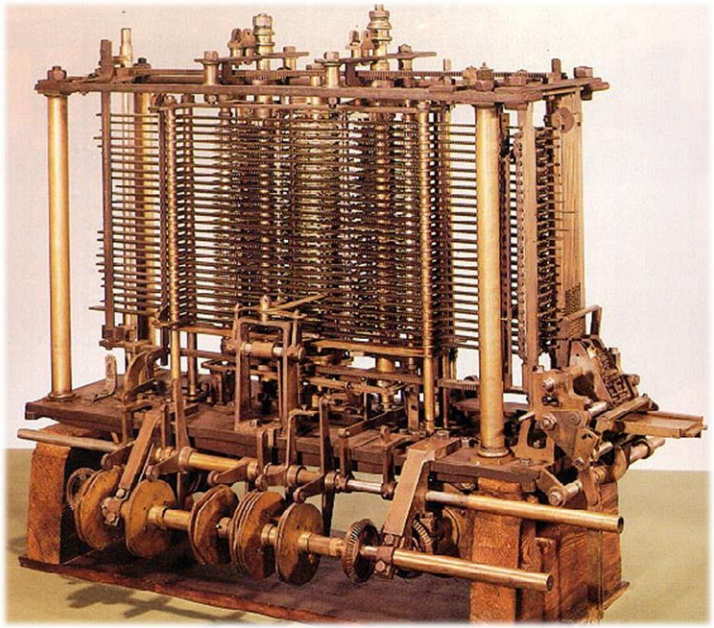
Mecanismo completo de una rueda y de la correa



1671.
La **Máquina de Leibniz**
Perfecciona la Pascalina
Sumas / Restas / Multiplicaciones / Divisiones / Raíces Cuadradas

1703 – Leibniz propone el sistema binario
Se descarta porque tenemos 10 dedos para contar

DECIMAL	BINARIO					
	8421		8	4	2	1
0	0000		0	0	0	0
1	0001		0	0	0	1
2	0010		0	0	1	0
3	0011		0	0	1	1
4	0100		0	1	0	0
5	0101		0	1	0	1
6	0110		0	1	1	0
7	0111		0	1	1	1
8	1000		1	0	0	0
9	1001		1	0	0	1
10	1010		1	0	1	0
11	1011		1	0	1	1
12	1100		1	1	0	0
13	1101		1	1	0	1
14	1110		1	1	1	0
15	1111		1	1	1	1



30 mts – largo
10 mts - ancho

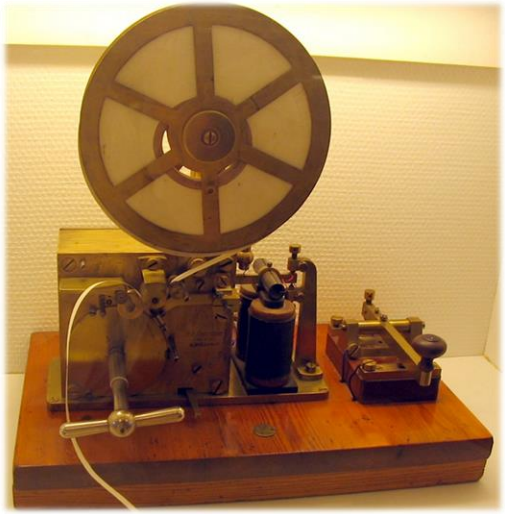
1833.
Diseño de la **máquina analítica** de **Charles Babbage**

Es capaz de ejecutar programas de computación

Hace uso por primera vez de tarjetas perforadas para controlar la máquina

En 1871 (su muerte) no se había podido fabricar por motivos políticos (fines bélicos)

1841 - Matemático inglés George Boole utilizó el **sistema binario** en ecuaciones algebraicas, estableciendo los fundamentos de lo que sería la **lógica de las computadoras**.



Emisor

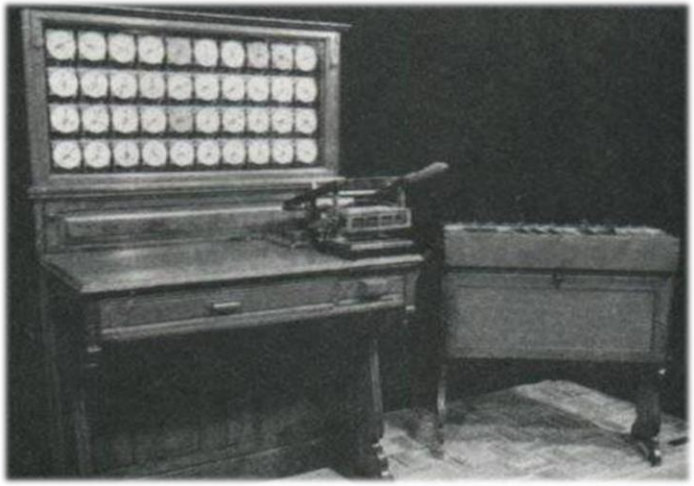
1837.
Morse crea el telégrafo
Primeras comunicaciones eléctricas

Canal

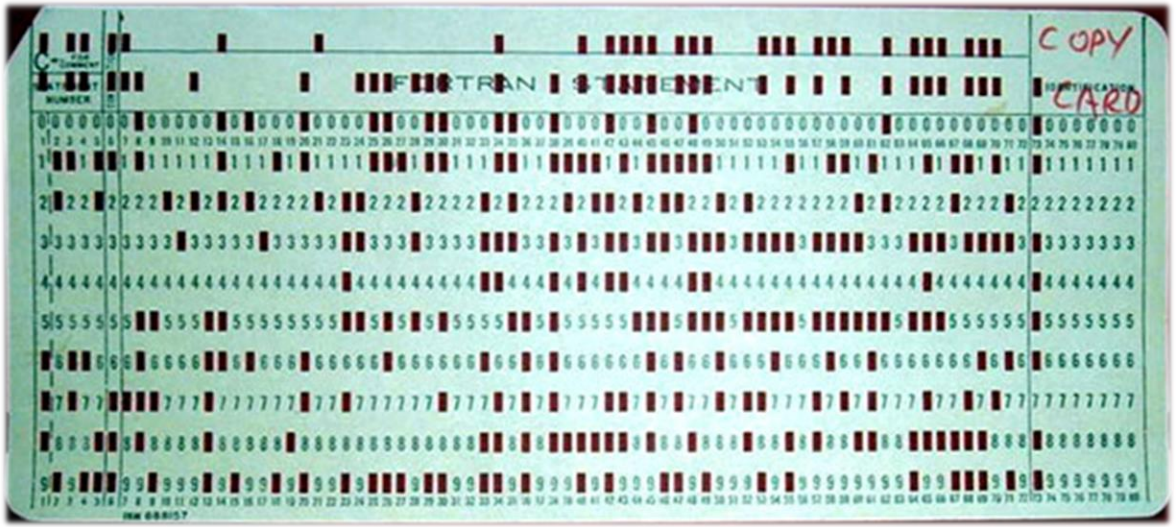
Receptor

HISTORIA TIC – Tecnologías de la Información y Comunicaciones

1876.
Alexander Graham Bell patenta el teléfono
Inventado por **Antonio Meucci**
Comunicación de masas a nivel Internacional



1890.
Hermann Hollerith (fundador de IBM - 1924)
Primera perforadora mecánica para representar letras y dígitos mediante **tarjetas perforadas**



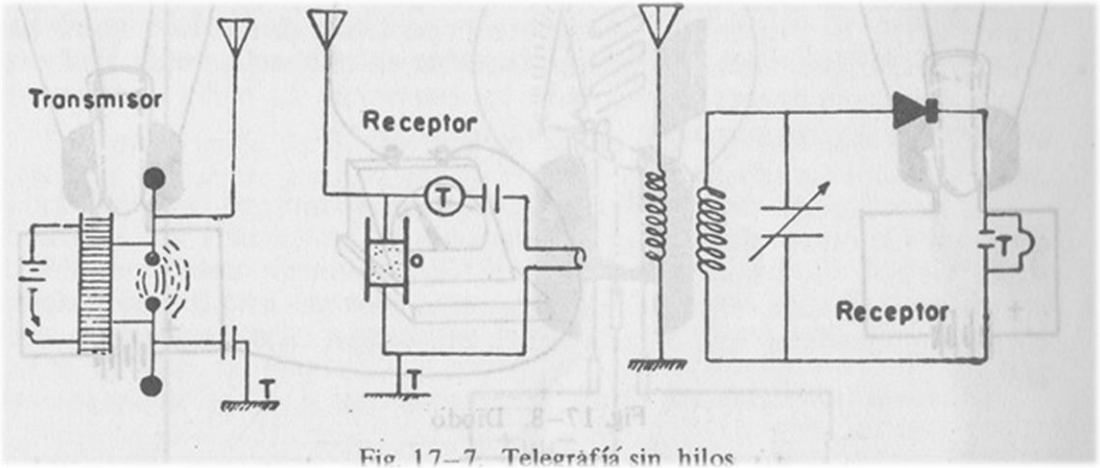
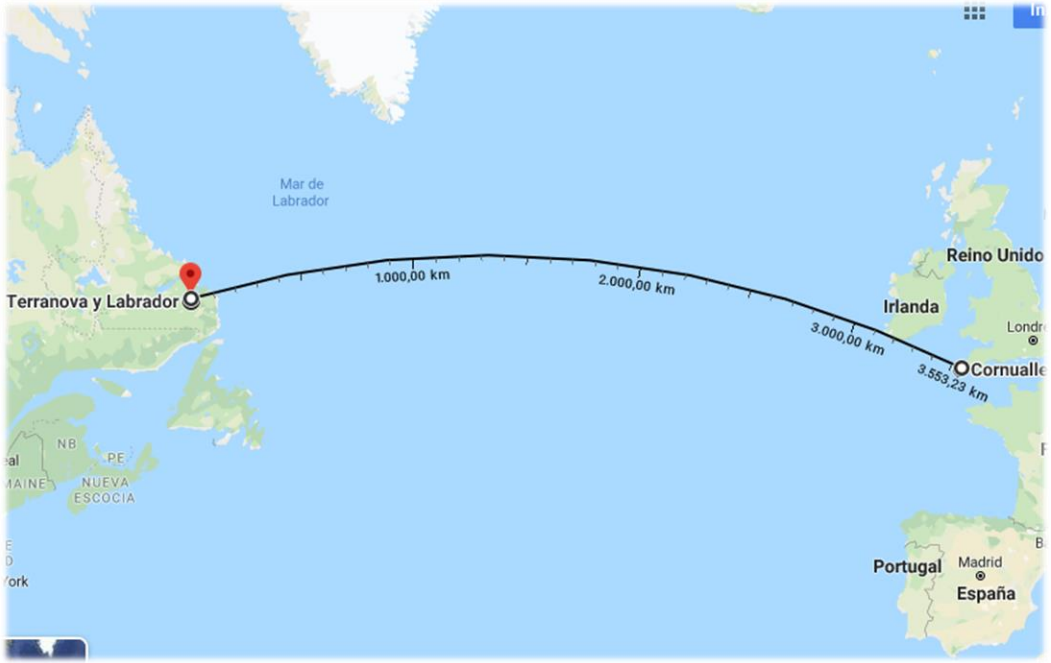


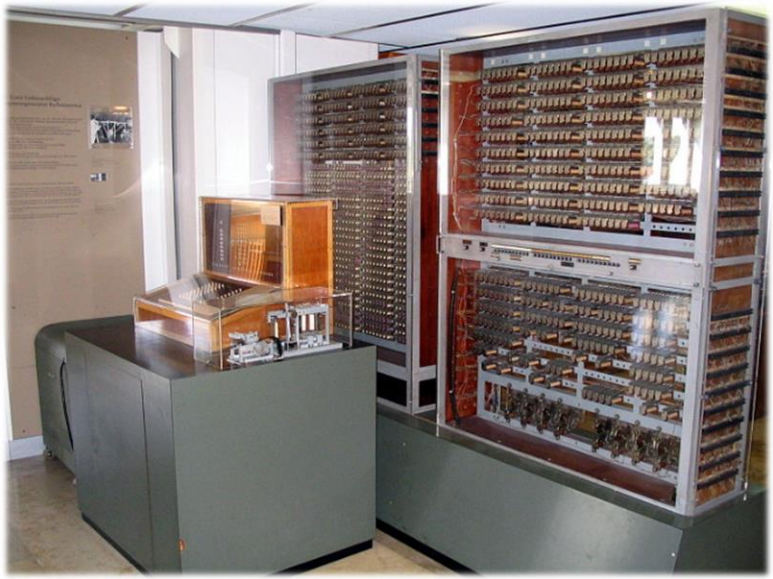
Fig. 17–7. Telegrafía sin hilos.

1901.
Marconi Telegrafía sin hilos o Radiotelegrafía

Primera transmisión desde Cornualles hasta Terranova

1906 Nochebuena.
Primera transmisión de radio

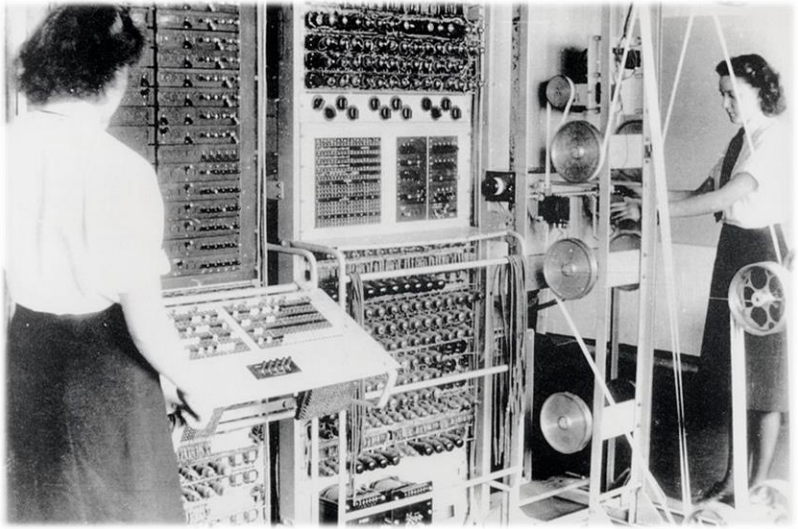




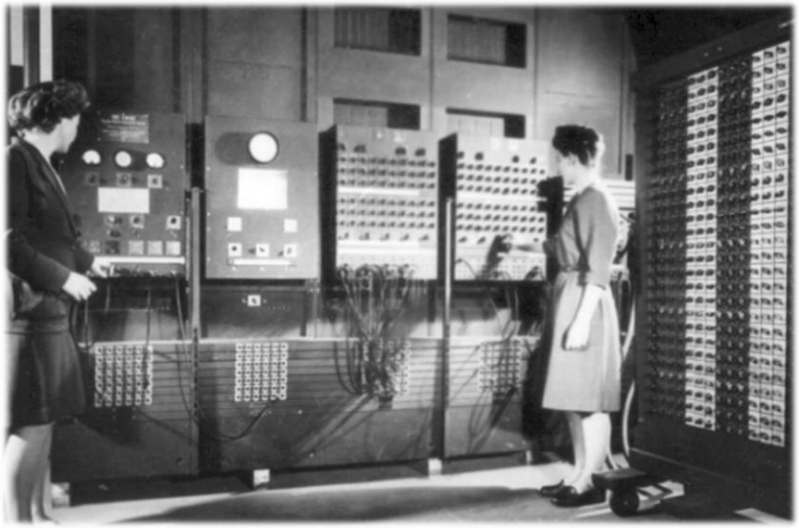
1941.
Konrad Suze Z3 primera computadora electromagnética programable con cinta perforadora

1943.
Alan Turing Colossus
Permite descifrar en unos pocos segundos los mensajes secretos de los nazis en la Segunda Guerra Mundial

Realizar una suma le costaba 0,7 segundos.
Una multiplicación o división le costaba 3 segundos

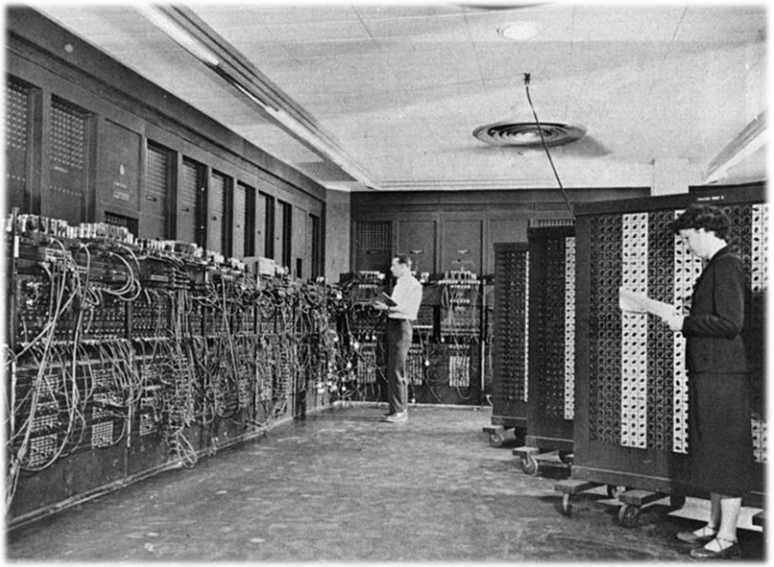


Primeros sistemas de defensa
CRIPTOANÁLISIS



1943.
John PresperEckert y John W. Mauchly
ENIAC
(Electronic Numerical Integrator And Calculator)
Primer ordenador electrónico y reprogrammable

Fue programado por 6 mujeres
- Primeras rutinas
- Primeras aplicaciones de software
- Primeras clases de programación



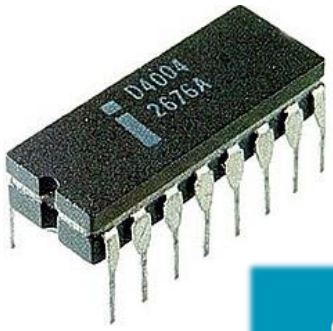
HISTORIA TIC – Tecnologías de la Información y Comunicaciones

1951.
UNIVAC-I Primer ordenador comercial

Primer cliente:
Oficina del Censo de Estados Unidos

1957.
FORTRAN Primer lenguaje de programación
1958
BELL - Primer **modem** – Bits por líneas analógicas
1961
Primera teoría de la **conmutación de paquetes**
1962
ARPA – Agencia de Proyectos de Investigación Avanzada - Idea de Red de ordenadores global
1969
ARPANET – 4 Universidades conectadas
Nace **UNIX**

HISTORIA TIC – Tecnologías de la Información y Comunicaciones



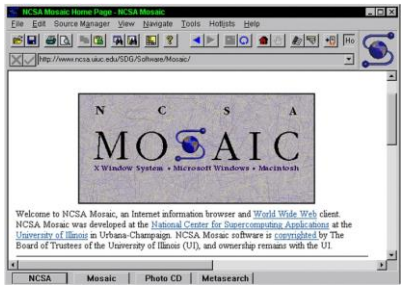
1971.
Intel 4004 – Primera CPU
IBM – **Primer disco 5 ¼**
ARPANET – 23 ordenadores conectados y primer email

1973.
NORUEGA e INGLATERRA se unen a través de INTERNET
1975
Steve Jobs y Steven Wozniak - nace APPLE I
Nace BASIC
Bill Gates y Paul Allen – MICROSOFT
1977
Tandy crea el TRS 80 I con periféricos externos
1978
COMMODORE – El ordenador de sombremesa más vendido a nivel mundial

HISTORIA TIC – Tecnologías de la Información y Comunicaciones

1981
IBM 5150 – Primer Personal Computer
Se define TCP/IP y nace la palabra INTERNET
1983
Primer DNS
Primer teléfono móvil Motorola El ***DynaTAC 8000X***

1984 – 1000 ordenadores conectado a Internet
1987 – 10.000 ordenadores conectado a Internet
1989 – 100.000 ordenadores conectado a Internet
Prototipo de WWW
1990 – Desaparece ARPANET
1991 – Se hace oficial el uso de WWW
Primera transmisión por Fibra Óptica – 4GBps
1992 – 10^6 ordenadores conectados a Internet
Motorola crea el primer móvil digital portátil.
1993 – Primer navegador MOSAIC
WANDEX primer buscador de Internet
IBM Simon primer móvil con funciones PDA
Primer libro digital – "*Del asesinato*"
1994 – Buscadores WebCrawler, Lycos y Excite!

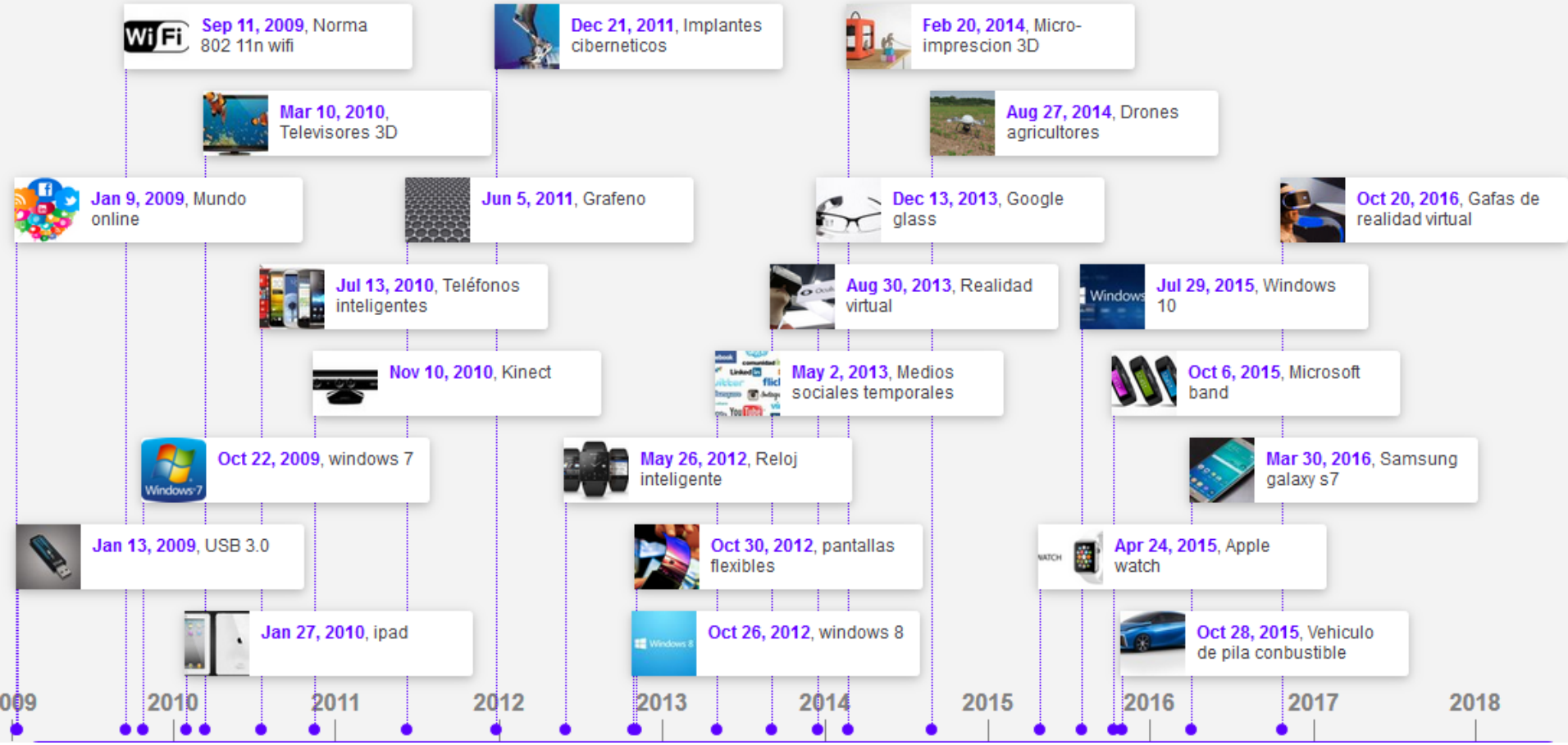


HISTORIA TIC – Tecnologías de la Información y Comunicaciones

1995 – Nacen los buscadores AltaVista y Yahoo!
1996 – 10^7 ordenadores conectados a Internet
Nokia 9000 Communicator primer smartphone con CPU Intel 386

1997 – Nace Google
1998 – *Rocket ebook* y *Softbook* – dos lectores de libros electrónicos
2001 – SixDegrees primera red social
2003 – Linkedin – Primera red social profesional
2004 – Facebook
2005 – Youtube
2006 – Twitter
2007 – Nace el iPhone
2009 – Whatsapp
2010 – Instagram

HISTORIA TIC – Tecnologías de la Información y Comunicaciones



- Blackphone: el smartphone ultrasecreto
- Un nuevo mapa del cerebro humano
- Baterías de larga duración
- Impresión 3D
- TV 4K – 8K

- Drones
- IoT
- Coches inteligentes autodirigidos
- BlockChain
- Realidad aumentada – Realidad Virtual

TIC – AMENAZAS

Físicas

Radiaciones electromagnéticas – Teclados inalámbricos, Radio Enlaces, Wifi sniffers, …

Puntos de conexión física no controlados.

Humedad, temperatura, calidad eléctrica, …

Sistemas de control de acceso a personal.

Lógicas

Sin intención

Vulnerabilidades en la programación, en el Sistema Operativo, en el Firmware (bugs, exploits).
Configuraciones incorrectas (firewalls, routers, switches, APs, …)

Con intención

Malware (virus, backdoors, troyanos, spyware, keyloggers, dialers, …)

Usuario

Trabaja con la información y con la infraestructura que la almacena, procesa y transmite

Amenaza activa

Empleado descontento
Crackers para romper el sistema o robar información
Gobiernos

Amenaza pasiva

Usuarios que ponen en riesgo la información sin conocimiento
¡Concienciación!. ¡Concienciación!.
¡Concienciación!. ¡Concienciación!.

ANÁLISIS DE RIESGO
PORCENTAJE DE RIESGO
UMBRAL DE RIESGO ADMISIBLE

PRINCIPALES AMENAZAS EN LA RED

Instituto Europeo de Estudios Empresariales S.A.
https://revistadigital.inesem.es/informatica-y-tics/las-principales-amenazas-la-red/

Ransomware

- Servicio Nacional de Salud de Gran Bretaña
- Red ferroviaria de San Francisco
- FedEx

Objetivos principales – Datos en la nube (Google, Amazon, IBM) – Grandes barreras -> Pequeñas empresas

EL PAÍS TECNOLOGÍA

MÓVILES REDES SOCIALES BANCO DE PRUEBAS RETINA MERISTATION

ATAQUE INFORMÁTICO ›

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

May: Es "un ataque internacional en el que varios países y organizaciones se han visto afectadas"

160

PABLO GUIMÓN

Londres - 12 MAY 2017 - 23:11 CEST

PRINCIPALES AMENAZAS EN LA RED

Instituto Europeo de Estudios Empresariales S.A.

https://revistadigital.inesem.es/informatica-y-tics/las-principales-amenazas-la-red/

JP Morgan reconoce que les hackearon 76 millones de cuentas en agosto

Entre la información a la que sí accedieron los hackers figuran nombres, direcciones, números de teléfono y direcciones de correo electrónico de sus clientes, así como información interna de la institución.
El banco JP Morgan Chase fue una de las cinco entidades estadounidenses víctimas de un ataque, cuyo fin aún se desconoce

LA INFORMACIÓN
Viernes, 03 Octubre 2014, 00:00

Violación de datos masivos

RGPD: violación de la seguridad de los datos personales es

*"**toda** violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos **datos**"*

que pueda producirse en cualquier fase del tratamiento: obtención, acceso, intervención, transmisión, conservación o supresión de datos.

Julio/2017 Uno de los mayores ciberataques de la historia. **76 millones de usuarios** y **7 millones de pequeñas empresas** clientes de JP Morgan Chase, fueron comprometidas por una violación de datos masivos.

PRINCIPALES AMENAZAS EN LA RED

Instituto Europeo de Estudios Empresariales S.A.

https://revistadigital.inesem.es/informatica-y-tics/las-principales-amenazas-la-red/

Ataques contra infraestructuras

¿Cuáles son sus ambiciones?

75% de los ciberataques tienen objetivos económicos.

Normalmente a Infraestructuras Críticas suelen ser intereses políticos o sociales

Medios:

- ***Corrupción de memoria***
- ***Accesos de administrador mal gestionados en sus sistemas***
- ***Controlar el ordenador conectado a los Controladores Lógicos Programables (PLC)***

BOLETÍN OFICIAL DEL ESTADO

Núm. 233 Martes 29 de septiembre de 2015 Sec. I. Pág. 87106

I. DISPOSICIONES GENERALES

JEFATURA DEL ESTADO

10389 *Ley 36/2015, de 28 de septiembre, de Seguridad Nacional.*

FELIPE VI

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

Índice

Preámbulo.
Título preliminar. Disposiciones generales.
Título I. Órganos competentes de la Seguridad Nacional.
Título II. Sistema de Seguridad Nacional.
Título III. Gestión de crisis en el marco del Sistema de Seguridad Nacional.
Título IV. Contribución de recursos a la Seguridad Nacional.

PREÁMBULO

I

La seguridad constituye la base sobre la cual una sociedad puede desarrollarse, preservar su libertad y la prosperidad de sus ciudadanos, y garantizar la estabilidad y buen funcionamiento de sus instituciones.

La legislación española así lo reconoce e interpreta, y contiene instrumentos normativos que, partiendo del marco diseñado por la Constitución, regulan los aspectos fundamentales que han venido permitiendo a los poderes públicos cumplir con sus obligaciones en esta materia.

PRINCIPALES AMENAZAS EN LA RED

Instituto Europeo de Estudios Empresariales S.A.

https://revistadigital.inesem.es/informatica-y-tics/las-principales-amenazas-la-red/

Criptomonedas mineras - Cryptojacking

Medio: Ordenadores infectados (Botnets) capaces de minar cryptomonedas

Usan el llamado Blockchain o Cadena de bloques. Una base de datos distribuida y descentralizada donde cada bloque está vinculado con el anterior y no puede ser modificado debido al Sellado de Tiempo.

Zcash y Monero son las monedas más habituales, ya que sus transacciones garantizan el anonimato de los atacantes.

¿Cómo infectan los equipos?

Esta infección instala software de extracción de bitcoins y sólo resulta perceptible para el usuario cuando nota un descenso en el rendimiento de su equipo.
Normalmente el proceso se lleva a cabo mediante adware capaces de instalar el software encargado de minar las criptomonedas. Cuando se haya creado una moneda, automáticamente se enviará a la cartera de los ciberdelincuentes.

"Parece incluso que los delincuentes prefieren el cryptojacking al ransomware".

PRINCIPALES AMENAZAS EN LA RED

Instituto Europeo de Estudios Empresariales S.A.

https://revistadigital.inesem.es/informatica-y-tics/las-principales-amenazas-la-red/

Amenazas cibernéticas en procesos de elecciones

Son ataques que se realizan desde un país a otro a través de redes informáticas e Internet. Tienen la intención de realizar una campaña de influencia sobre la opinión pública con objetivos que denigren a uno de los candidatos que participa en esas elecciones. Utilizan noticias falsas que le perjudiquen en la carrera electoral. Consiguen alterar el resultado las elecciones para lograr un beneficio o perjudicar a un país rival.

URUGUAY ›

Las 'fake news' ensucian la campaña electoral en Uruguay

Los partidos tradicionales acusan al millonario Juan Sartori, un recién llegado a la política que crece en los sondeos como precandidato de la derecha

MAGDALENA MARTÍNEZ

Montevideo - 23 JUN 2019 - 14:22 CEST

El precandidato a presidente de Uruguay, Juan Sartori, saluda durante un mitin de campaña en marzo pasado. AFP

NEWSLETTER

Recibe el boletín de América

TE PUEDE INTERESAR

El presidente de Uruguay anuncia que tiene un "nódulo pulmonar con características malignas"

La tensión entre Argentina y Brasil lastra la cumbre de presidentes del Mercosur

Un sindicato de Mossos hackeado paga una multa e indemniza a varios agentes

La respuesta del Derecho frente a los ataques 'ransomware'

PRINCIPALES AMENAZAS EN LA RED

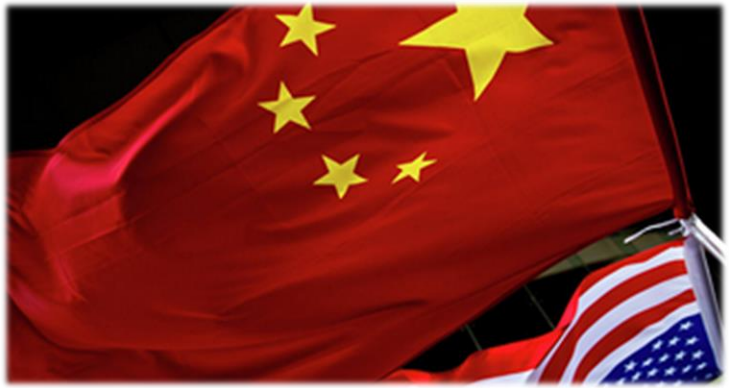
Instituto Europeo de Estudios Empresariales S.A.

https://revistadigital.inesem.es/informatica-y-tics/las-principales-amenazas-la-red/

Militarización de la Inteligencia Artificial

El avance tecnológico en manos de la ciberdelincuencia.

Los modelos de aprendizaje automático ahora pueden unir a los humanos en el arte de elaborar mensajes falsos convincentes, y pueden producir muchos más sin cansarse.
Los hackers se aprovecharán de esto para impulsar más ataques de phishing. También es probable que usen la inteligencia artificial para ayudar a diseñar malware que sea aún mejor para engañar a las “cajas de arena” o los programas de seguridad que intentan detectar el código malicioso antes de implementarlo en los sistemas de las empresas.



Detrás de las amenazas de guerra comercial entre EEUU y China se encuentra el posicionamiento tecnológico que marcará el siglo XXI sobre la primacía global de la inteligencia artificial cuando Pekín ha proclamado que será el líder indiscutible en 2030.

PRINCIPALES AMENAZAS EN LA RED

Chinese Attackers Hacked Forbes Website in Watering Hole Attack: Security Firms

By Fahmida Y. Rashid on February 11, 2015

Share 18 G+1 0 Tweet Recomendar 22 RSS

A Chinese attack group infected Forbes.com back in November in a watering hole attack target
two se

"A Chi
style v
Novem

The at
the otl
released Tuesday. Adobe fixed the flaw back in Decemb
Explorer as part of its Patch Tuesday release.

The cyber-espionage campaign appeared to last only a f
not rul

The ma
whene
than tc
typical
for ma
said St
becaus

Se duplican incidentes ciberseguridad en las grandes empresas estratégicas

EFE 16/11/2017 (15:54)

Anonymous
@Anonymous_opt
Seguir
La web de la Casa Real está siendo atacada.
Inestable casareal.es#AnonymousOperation #OpCatalunya
9:51 - 25 oct. 2017
82 713 1.799

US authorities name five Chinese military hackers wanted for espionage

31 charges brought against alleged PLA hacking team

By Iain Thomson, 19 May 2014 Follow 2,251 followers

PRINCIPALES AMENAZAS EN LA RED

incibe-cert_

Alerta ▾ Incidentes ▾ Servicios

Incidente de seguridad relacionado con antivirus en SCI

Todos sabemos que es imposible hablar de una seguridad que sea infalible y con los antivirus no iba a ser menos, esto se puso de manifiesto en 2014, cuando un fabricante procedente de China incorporó el malware ZombieZero en dispositivos portátiles de lectura de códigos de barras y en sus actualizaciones, lo cual les permitió robar información de sus clientes.

Esto sirvió para que las empresas tomasen más precauciones al tratar con los proveedores o fabricantes e implementasen más criterios de seguridad antes de actualizar los dispositivos, además de analizar periódicamente todos los dispositivos que se obtienen o actualicen con los respectivos antivirus.

Como solución para este incidente, podría haber sido suficiente un antivirus que comprobase que tanto las actualizaciones recibidas como los nuevos productos estaban libres de malware.

Tu socio tecnológico

nunsys®

COMUNICACIONES · SISTEMAS · SOFTWARE · MARKETING · FORMACIÓN

economistas
Colegio de Valencia

Principales ataques cibernéticos

Repercusión económica

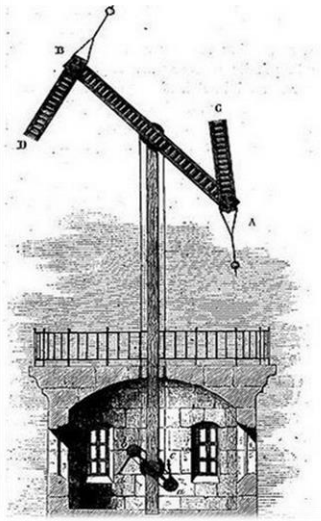
2

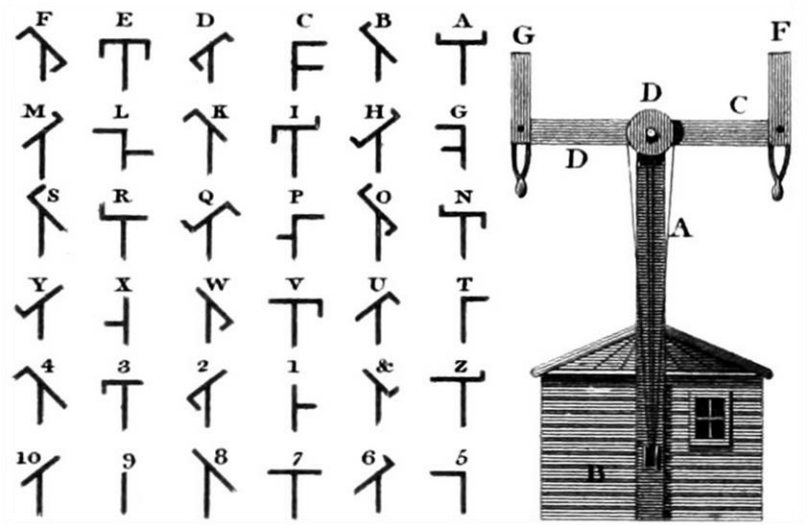
PRINCIPALES ATAQUES CIBERNÉTICOS

PRIMER CIBERATAQUE REGISTRADO
Ataque al telégrafo óptico francés hace 200 años
1834 banqueros corruptos François y Joseph Blanc – Intercambio de bonos del gobierno – obtención anticipada de información privilegiada

Sistema telegráfico reservado al gobierno francés, consistente en una cadena de torres con brazos ajustables.
Las diferentes configuraciones de estos brazos correspondían a letras, números y otros signos.

Soborno al operador (**factor humano**) de telégrafos de la ciudad de Tours
Introducción de mensajes ocultos (**integridad**)
Operador en Bourdeos observando y transmitiendo la información a los Blanc
1836 descubiertos al enfermar el operador sobornado. No leyes redes de datos. No inculpados.





Fte-https://www.nobbot.com

PRINCIPALES ATAQUES CIBERNÉTICOS

VIRUS

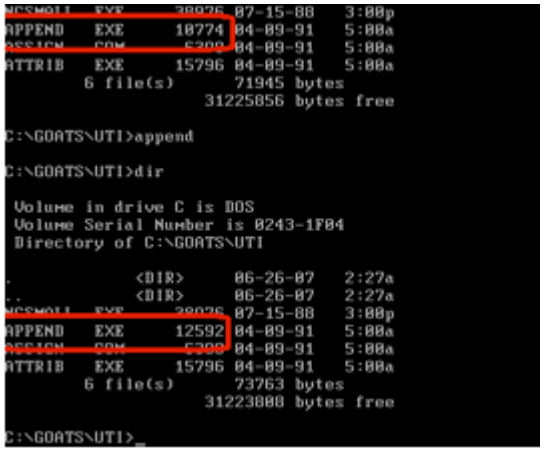
Viernes 13 / Jerusalem
Se ejecutaba todos los viernes 13 autoinstalándose en la RAM
Modificaba todos los archivos .com y .exe aumentando su tamaño
Objetivo:Colapsar los equipos. SO – MsDOS

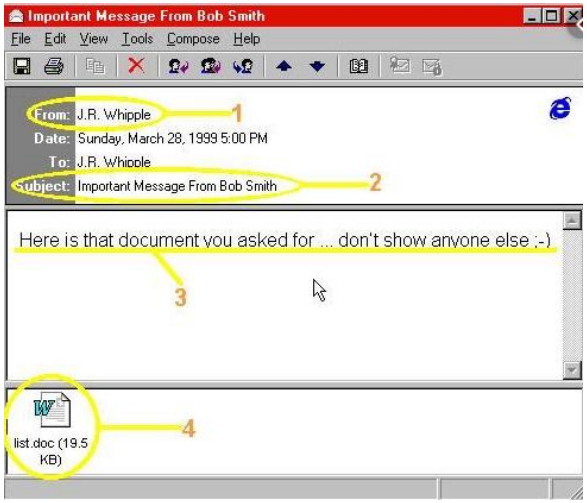
Melissa - 1999
Primer virus que se propagaba a través del email
Venía insertado en documentos Word y Excel
Gancho – Claves de acceso a páginas web eróticas

I love you – 2000
Email con título “I love you” y con adjunto “Love letter for you”
Destrucción de archivos y reenvío a contactos
Impacto - > $45*10^6$ ordenares infectados

SASSER – 2004
Vulnerabilidad de Windows
Inutilizaba el equipo – Afectó a todo tipo de empresas

Conficker – 2008
Vulnerabilidad de Windows
Infección de equipos . Envío de datos personales a servidor
Actualizaciones desactivadas y AV sin acceso





Fte-https://www.nobbot.com

PRINCIPALES ATAQUES CIBERNÉTICOS

El coste medio de un ciberataque empresarial supera los tres millones

https://www.expansion.com/andalucia/2019/02/20/5c6c6753e2704ebb318b45ea.html

El jefe de Ciberseguridad del CNI advierte que las empresas y las administraciones públicas apenas rozan el aprobado en el cumplimiento de la última ley de protección y seguridad.

El **coste medio** de una brecha de seguridad se sitúa en más de **3 millones de euros** y **todas** las **empresas** están **amenazadas**, independientemente de su tamaño. **Todas las compañías** han sido **hackeadas**, pero algunas lo saben y otras no.

Según las estadísticas del **Ministerio de Interior** durante el año **2017** se conocieron **81.307 delitos** informáticos en España, lo que supone un fortísimo **crecimiento** respecto al año anterior, un **22,1% más**.

PRINCIPALES ATAQUES CIBERNÉTICOS

https://www.elconfidencialdigital.com/articulo/te_lo_aclaro/coste-ciberataques/20180104235335087965.html

El **Foro Económico Mundial** incluye desde 2014 los ciberataques como uno de los **cinco riesgos globales más importantes**, en términos de probabilidad, junto al cambio climático, el desempleo o las catástrofes naturales.

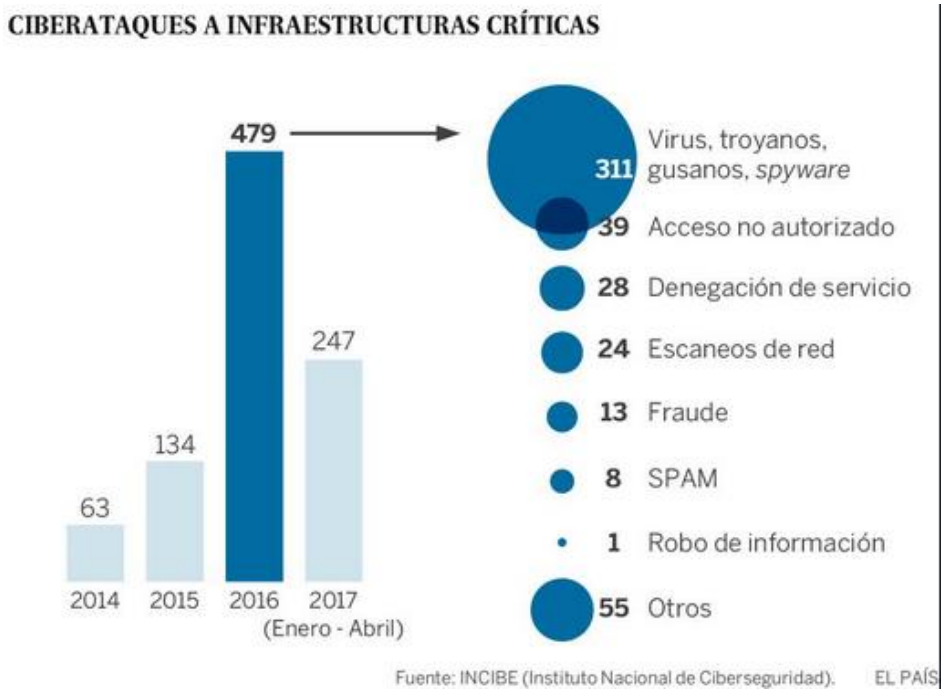
Además, según un estudio elaborado por McAfee se estima que el **cibercrimen** tiene un **impacto global en la economía** de entre 350.000 millones y un billón de euros al año, cerca del **1% del PIB mundial**.

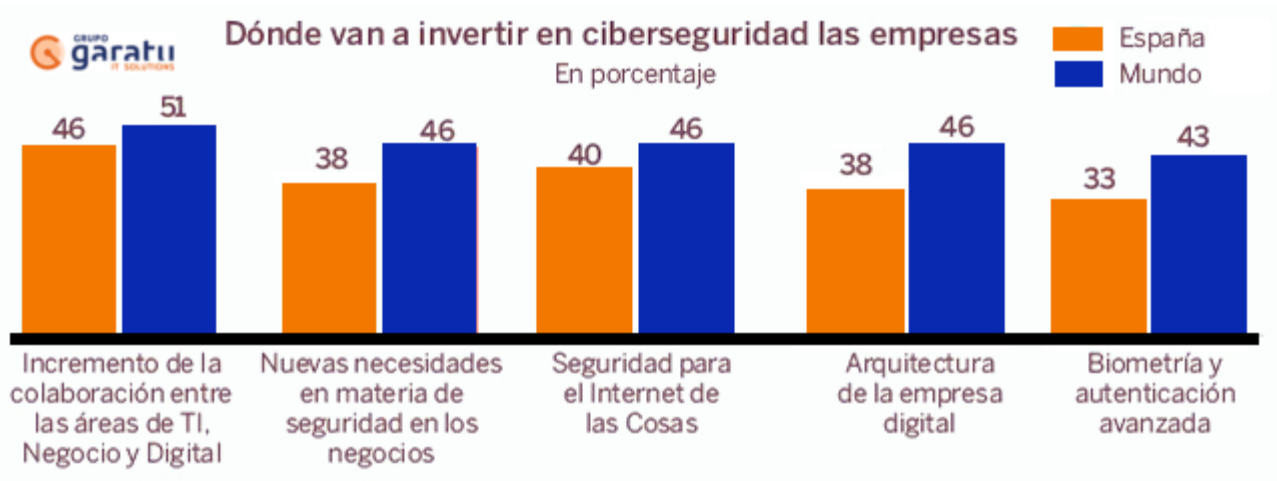
Sólo en España, el pasado año el **coste medio** de un ciberataque rondó los **75.000 euros**, lo que supone unos **14.000 millones** para las empresas del país, según cifras del Instituto Nacional de Ciberseguridad (**INCIBE**).

Asegura también que a **diario** son atacados entre **100.000** y **120.000** equipos en **España**

Google eliminó 58,8 millones de anuncios phising en 2018
https://ipmark.com/google-elimino-588-millones-anuncios-phising/

PRINCIPALES ATAQUES CIBERNÉTICOS





Consejo Europeo
Consejo de la Unión Europea

Ciberataques: el Consejo ya puede imponer sanciones

El 17 de mayo de 2019, el Consejo ha establecido un marco que permite a la UE imponer **medidas restrictivas específicas para disuadir y contrarrestar los ciberataques** que representen una **amenaza exterior para la UE o sus Estados miembros**, en particular los perpetrados **contra terceros Estados u organizaciones internacionales**, cuando esas medidas se consideren necesarias para alcanzar los objetivos de la política exterior y de seguridad común (PESC).

UE imponer sanciones

- personas o entidades **responsables de ciberataques o tentativas de ciberataques**
- que prestan para ello **apoyo** financiero, técnico o material
- están **implicadas** de algún otro modo
- las personas y entidades asociadas con ellas

Entre las medidas restrictivas figuran:

- **inmovilización de activos** de dichas personas y entidades
- **prohibición** de viajar a la UE
- las personas y las entidades de la UE tienen prohibido poner fondos a disposición de aquellas que figuren en la lista

Tu socio tecnológico

nunsys®

COMUNICACIONES · SISTEMAS · SOFTWARE · MARKETING · FORMACIÓN

economistas
Colegio de Valencia

Principales métodos de ataque

Cómo paliarlos

ATAQUES POR TIPOLOGÍA

PHISHING – Suplantación de identidad
Se consigue suplantar la identidad (engañando o robando la identidad real) y se aprovecha para conseguir que la persona engañada realice acciones que nos permitan tomar el control del dispositivo / sistema.
Medios: email / Ingeniería Social

DDoS – Denegación de servicio distribuido
Se genera una cantidad suficiente de tráfico sobre el objetivo para dejarlo fuera de servicio. Se compromete a la organización impidiendo el acceso al servicio.

Drive-byDownload – Instalación involuntaria de software malintencionado
Se consigue realizar una descarga de un software malintencionado sin consentimiento del propietario. Normalmente al hacer 'clic' en un enlace indebido, pero también puede entrar por otro medio distinto a Internet. Este malware es la puerta de entrada al cracker - **Troyano**

APT – Ataques de Amenazas Persistentes
New York Times -> divulgación de ataque por parte de unidad militar china (APT1) contra redes concretas de diferentes medios mediante spear phishing y malware
Objetivos concretos

ATAQUES POR TIPOLOGÍA

RAMSOMWARE
El objetivo es el secuestro del dispositivo y/o de su información para solicitar un rescate.

CRYPTOJACKING
Robo de recursos para obtención de beneficios por minería de cryptomonedas

SPEAR PHISING
Estafa de correo electrónico o comunicaciones dirigida a personas, corporaciones u organizaciones. Es muy parecido al phishing «tradicional». En lugar de realizar grandes ataques, mirando a grupos de personas y empresas diversas, esta variación de phishing hace el robo de información específica de organizaciones precisamente seleccionadas.

CASOS REALES

A nivel gubernamental

Fte-https://www.nobbot.com

CIBERATAQUES – CASOS REALES – NIVEL GUBERNAMENTAL

CIBERGUERRAS – PAISES ENFRENTADOS

US joins UK in blaming Russia for NotPetya cyber-attack

White House labels Kremlin 'reckless', while UK says it 'undermined democracy'

US accuses Russia of cyber-attack on energy sector and imposes new sanctions

US officials say malware was found in operating systems of several US energy companies and announce sanctions for election interference

Full details on the sanctions

CYBER RISK

EU agrees to use sanctions against cyber hackers

Reuters Staff

LUXEMBOUR
caught attacki
bloc's latest st

DEPORTADOS CUATRO AGENTES DEL KREMLIN

Reino Unido, Holanda y EE.UU. acusan a Rusia de ciberataques a escala global

• El Gobierno británico acusa a los servicios secretos rusos de llevar a cabo una serie de ataques con 'ransomware' mundiales

AGENCIAS, LA HAYA / LONDRES / WASHINGTON

Fte-https://www.nobbot.com

CIBERAMEZANAS INTERNACIONALES – TRES CATEGORÍAS

- ❑ **Sabotaje**
- ❑ **Espionaje**
- ❑ **Subversión**

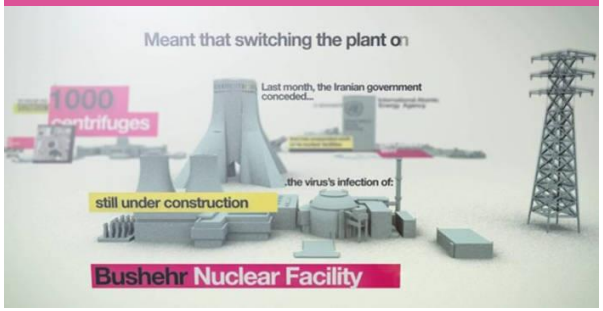
Sabotaje

Éxito => Requiere de gran cantidad de recursos y alto grado de sofisticación técnica.

STUXNET

Central nuclear
Irán

Stuxnet
Centrifugadoras de Uranio
"El virus que toma el control de las máquinas y les ordena autodestruirse"



Ataque dirigido

- Distribuido por USB
- Conocedores del objetivo
- Crackers específicos
- Controlador de Siemens
- Sospecha de fines políticos EEUU + Israel → Irán
- Riesgo nuclear
- Retraso de 2 años en avance nuclear de Irán

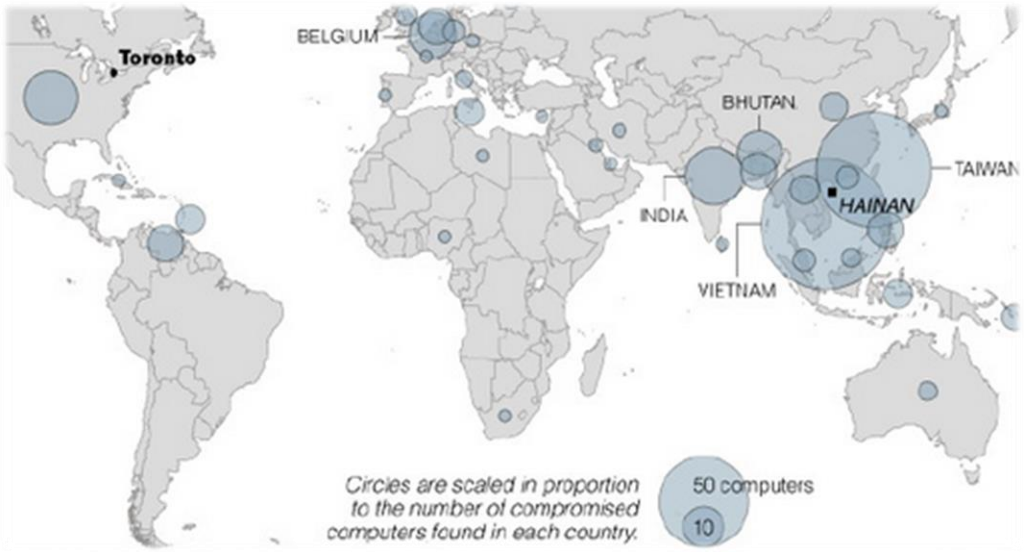
CIBERAMEZANAS INTERNACIONALES – TRES CATEGORÍAS

- ❑ **Sabotaje**
- ❑ **Espionaje**
- ❑ **Subversión**

Espionaje

Éxito => Complicidad gubernamental.

GHOSTNET



Ciberherramienta descubierta en 2009 que ha infectado a más de un centenar de ordenadores de diversos ministerios de exteriores, embajadas, organizaciones internacionales, medios de prensa y organizaciones no gubernamentales de 130 países.

El virus podría enviar documentos de los discos duros de los ordenadores infectados a su creador, grabar las pulsaciones del teclado de los usuarios, y activar la cámara y micrófono del ordenador infectado

CIBERAMEZANAS – TRES CATEGORÍAS

- ❑ **Sabotaje**
- ❑ **Espionaje**
- ❑ **Subversión**

Subversión

Éxito => Activistas → Minar la reputación y confianza

ANONYMOUS - Anonymusse

2011 empresa estadounidense de seguridad tecnológica **HBGary Federal**, clientes:

- Gobierno de los Estados Unidos
- McAfee

Afirmó poseer información que identifica a un notorio grupo de hackeractivistas, conocidos como Anonymus.

Respuesta, **Anonymusse**

- se infiltró en los servidores de HBGary, publicando 40 mil correos electrónicos privados
- tumbaron su sistema telefónico
- Crackearon la cuenta de Twitter del Jefe Ejecutivo de la empresa y publicaron su número de la seguridad social en Internet

Los ataques subversivos, en realidad no representan una amenaza que se pueda considerar catastrófica, por ello se considera de bajo impacto económico directo

Anonymous hackea la web de Vox y accede a los datos de 30.000 usuarios

20MINUTOS.ES 13.12.2018 - 11:06H

Este verano el grupo tumbó durante unas horas las webs del PSOE, la Policía y el Constitucional.

2016. "Shadow Brokers" proclamó haber sido **los primeros en acceder a la Agencia de Seguridad Nacional de los Estados Unidos**, más conocida como la NSA. El grupo filtró toda una serie de exploits que posteriormente fueron utilizados para realizar múltiples ataques, como fue el caso del asunto "**WannaCry**" basado en el exploit "**EternalBlue**" que la propia NSA llegó a utilizar.

Fte-https://www.nobbot.com

CASOS REALES

A nivel empresarial

Fte-https://www.nobbot.com

Ejemplo 1: CIBERESPIONAJE INDUSTRIAL

La empresa X está detectando que las licitaciones a las que se presenta son siempre superadas por otra compañía (siempre la misma) y generalmente por pequeños matices presupuestarios. Sospecha que está siendo objeto de espionaje industrial o fuga de información en su seno.

¿Qué estaba pasando?

1. **Infección equipo interno no protegido (windows XP)**
2. **Comunicación con servidor para actualizar y propagarse sin ser detectado (convertirse en APT)**
3. **Programación de APT personalizada para infectar ficheros Excel de presupuestos, programas…**
4. **Captura de cada presupuesto enviado por cualquier empleado a un servidor externo**
5. **Presentación de oferta mejorada al cliente final**

Medidas

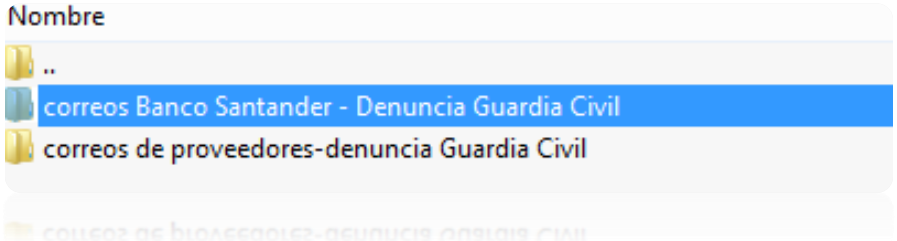
1. **Peritaje informático y análisis forense**
2. **Actualización de equipos**
3. **Endpoint de pago actualizado**
4. **Aumentar el nivel de control en la seguridad perimetral – Equipos UTM**
5. **Seguridad gestionada**

Ejemplo 2: CIBERESPIONAJE INDUSTRIAL

La empresa X sufre un ataque de reputación. Sus clientes, bancos y proveedores reciben información clasificada intercambiada entre esta empresa y sus abogados para estudiar un posible cierre de la actividad.

¿Qué estaba pasando?

1. Acceso ilegal al correo de la empresa (Ataque a un webmail vulnerable)
2. Redirección o espionaje de correos
3. Creación de una cuenta anónima de correo
4. Envío de correos no rastreables a proveedores y clientes con información dañina, suplantando al gerente



Medidas

1. Peritaje informático y análisis forense
2. Proveedores de confianza (dominio)
3. Correo seguro (https) en un proveedor fiable
4. Web actualizada

Ejemplo 3: SUPLANTACIÓN DE IDENTIDAD

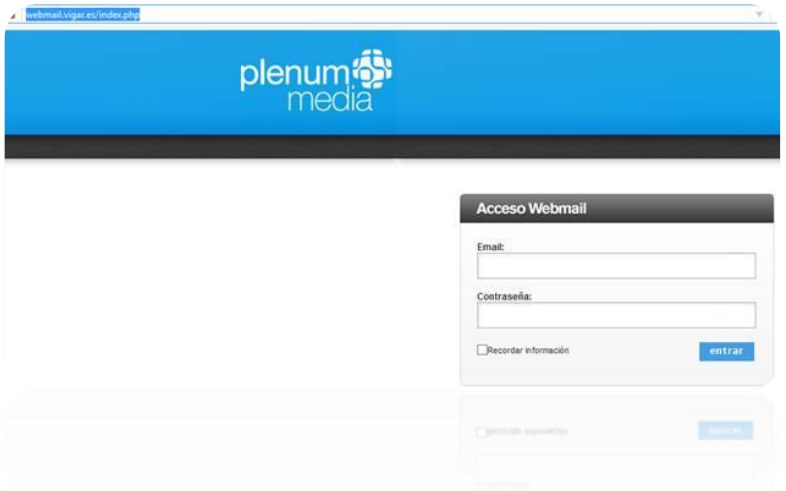
Una empresa trabaja con proveedores internacionales (especialmente fábricas en China). Recibe un correo de su proveedor "suplantado" con la factura del mismo, y un número de cuenta de pago diferente del habitual. El cliente paga y el rastro desaparece. El proveedor le reclama el pago en la cuenta habitual.

¿Qué estaba pasando?

1. Ataque a un correo vulnerable (del proveedor extranjero – del ISP del cliente)
2. Creación de una cuenta de correo similar a la del proveedor (o suplantando directamente)
3. Lo más complejo ha sido interceptar el correo original, y sustituirlo por uno cambiando el IBAN de pago
4. Envío de una orden de pago suplantando al departamento financiero

Medidas

1. Emplear contraseñas seguras
   https://haveibeenpwned.com/
2. Emplear canales seguros con proveedores
3. Cifrado de las comunicaciones
4. Autenticación de los usuarios
5. Usar canales seguros (https, correo seguro)
6. Doble factor de autenticación
7. Alertas de O365 ante accesos sospechosos



Ejemplo 4: EL FRAUDE DEL CEO

El "jefe" está de viaje de negocios (conferencia, visita a proveedores…). El director financiero recibe un correo "falso" del jefe solicitando acceso directo a la cuenta del banco, o transferencia urgente a un proveedor para empezar a trabajar con ellos.

¿Qué estaba pasando?

1. La empresa o el empresario ha publicado en redes sociales información del viaje
2. Un atacante recopila información crítica del viaje que emplear en la estafa
3. El atacante crea un correo similar al del empresario, y envía un correo al financiero solicitando credenciales de acceso a la cuenta del banco
4. El atacante opera en el banco transfiriendo fondos a cuentas protegidas

Medidas

1. Concienciar a los empleados (financiero, secretariado)
2. No publicar correos ni información crítica en redes sociales
3. Emplear correo seguro: AntiSPAM

Ejemplo 5: ACTIVIDAD ILÍCITA DE EMPLEADOS

Un gerente de tienda de una compañía de muebles está "revelando" información confidencial a socios para montar una empresa competencia de aquella en la que trabaja.

¿Qué estaba pasando?

1. Gerente de tienda crea otra marca
2. Tras despido, análisis Forense en su PC para investigar el incidente
3. Registros de llamadas desde su móvil corporativo a sus nuevos socios
4. Registro de conversaciones de Whatsapp con la traza de sus intenciones, gracias al backup en el PC
5. Registro de ficheros confidenciales copiados a disco duro externo

Medidas

1. Políticas de seguridad y sanción
2. Soluciones de control de la documentación (DLP)
3. Monitorización de la actividad del usuario

Ejemplo 6: RANSOMWARE

Un empleado abre un email malicioso (malware), y se infecta con el ransomware. Se propaga por su equipo y por los servidores de ficheros de la empresa. Ha cifrado información confidencial, alguna está en copias de seguridad, pero otra era en local.

¿Qué estaba pasando?

1. Correo por usuario vulnerable (recepción, financiero, etc.)
2. También por gerencia, o PC de un empleado que usa su familia
3. Infección de un equipo de la red industrial con parada de producción
4. Recuperación de copias de seguridad en servidores de ficheros
4. Pérdida de información de los PCs afectados / pago de rescato o ¿¿??
5. Abrir incidencia y conseguir vacuna a través de INCIBE
6. ¿Expedientar al empleado causante del incidente?

Medidas

1. Formación y concienciación
2. Protección antiransomware (Endpoint de pago con análisis de comportamiento)
3. Implementación de medidas de seguridad (guía CCN-STIC)
4. Campaña de Trading o simulación de Ransomware

DEFENSAS

Fte-https://www.nobbot.com

Conoce - Actúa

5 Consejos para reforzar la ciberseguridad

1 Asegúrate de que estás invirtiendo lo suficiente en ciberseguridad.

Algunas industrias, como los medios de comunicación y los mercados de consumo, están asignando menos y pueden estar más expuestas a los riesgos cibernéticos.

2 Piensa en la ciberseguridad como cualquier otra amenaza existencial para tu negocio.

Los riesgos no se limitan a la privacidad, la responsabilidad y el robo de datos; también pueden producirse enormes riesgos operativos si se interrumpe el negocio, con repercusiones en la reputación que pueden perjudicar las posiciones de mercado.

Fte-https://www.nobbot.com

3 Presta atención a los riesgos de los socios y su cadena de suministro.

A medida que las empresas recurren a ecosistemas de terceros para impulsar la transformación digital, aumentan su vulnerabilidad a los riesgos cibernéticos.

4 Ten en cuenta que los riesgos legales y regulatorios también están aumentando sustancialmente.

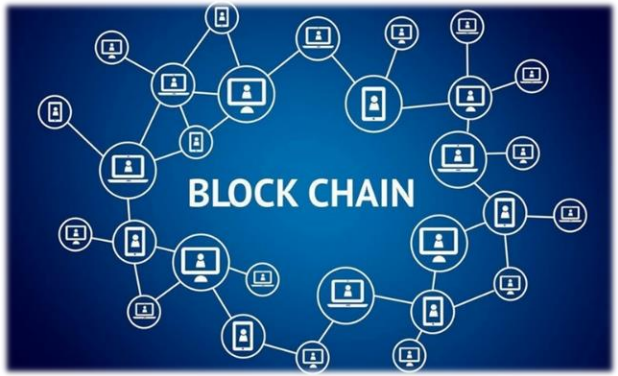
Las empresas que no cumplen con las nuevas normas se enfrentan a fuertes sanciones y consecuencias legales.

5 Mide sus pérdidas, costes y devoluciones totales.

Cuando seas golpeado por un ciberataque exitoso, necesitas entender todos tus costes – directos e indirectos, tangibles e intangibles.

https://www.directivosyempresas.com/empresas/impacto-economico-de-cibertataques/

Fte-https://www.nobbot.com



Transacciones actuales
Emisor – Receptor -> Fiabilidad
Punto único de almacenamiento de la información
Sistema centralizado

BLOCK CHAIN

Transacción = HASH

0x979a47cdd7afd0468b3b2cb0943a4ab54bfaec226462ec95b8f2cbad9df72dcb.

Transacciones con blockchain - **Libro de contabilidad** totalmente distribuido
BBDD de participación pública totalmente distribuida en la que se registran las transacciones..

Cada emisor de transacciones dispone de su clave privada y clave pública.
Clave privada: garantiza la identidad del usuario
Clave pública: permite mostrar aquello que desea enseñar al resto

Resistencia a la censura o al arbitraje
Descentralización absoluta
Ausencia de confianza en terceros
Globalidad y neutralidad
Transacciones encriptadas. Inalterables. Privacidad.

Primera aplicación – Criptomonedas

TIC – DEFENSAS

Según el Foro Económico Mundial, en los próximos años seremos testigos de una importante transformación en la que la blockchain acabará convirtiéndose en el "corazón" del futuro sistema financiero mundial.

Aunque el blockchain se creó de la mano de **Bitcoin**, las aplicaciones innovadoras de la cadena de bloques surgieron con **Ethereum**. Mientras que la blockchain de bitcoin limitaba su uso a aplicaciones financieras, la de ethereum permite correr pequeñas aplicaciones, conocidas como contratos inteligentes o *smart contracts*.

SECTORE PARA SU IMPLEMENTACIÓ:

- Salud y sanidad
- Criptomonedas
- Finanzas y economía
- Fintech y banca
- Big Data
- Notarios

- Firma digital y verificación de la identidad
- Logistica y transporte
- Internet de las cosas
- Alimentación y trazabilidad
- Turismo y hoteles
- Energía

- Seguros
- Abogados, derecho y sector jurídico
- Recursos Humanos
- RGPD
- Votaciones y elecciones
- Telecomunicaciones, …

LIBRA
La nueva cryptomoneda de Facebook

Calibra será una cartera digital que permitirá almacenar y utilizar la nueva moneda digital Libra. Es decir, una plataforma de pagos para **Facebook**, **Messenger** y **WhatsApp** que existirá como aplicación independiente en iOS y Android. Una cartera conectada para todo el mundo y multiplataforma, una cartera que permitirá enviar dinero rápidamente y estará basada en esta nueva moneda digital en la que ya nos explican desde el inicio que no se encontrará en manos de Facebook.

PUNTOS A CONSIDERAR

Fte-https://www.nobbot.com

TIC – DEFENSAS

> **Gestionar las TIC**
  - Infraestructura adecuada y correctamente implementada
  - Mantener y actualizar los activos – Routers – NG-UTM (FW) – Servidores/Equipos – Sistemas operativos
  - Aplicar políticas internas de seguridad – Accesos, contraseñas, tratamiento de la información
  - Tratamiento con terceros

> **Asegurar los hosts**

  Seguridad en el perímetro: FW

  Seguridad en el equipo: Endpoint

> **Realizar tests de intrusión periódicas**

  Hacking ético externo e interno

> **Disponer de un plan de continuidad de negocio**

  Planes de contingencia

  Remote Backup / Disaster Recovery

> **Complementar medidas de seguridad.**

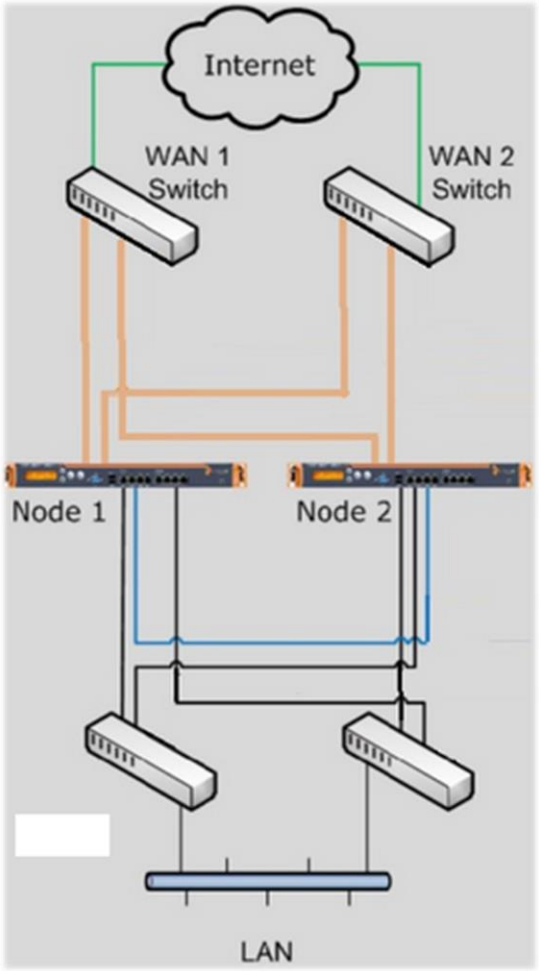
  Defensa en profundidad. Foros / Blogs relacionados con seguridad.

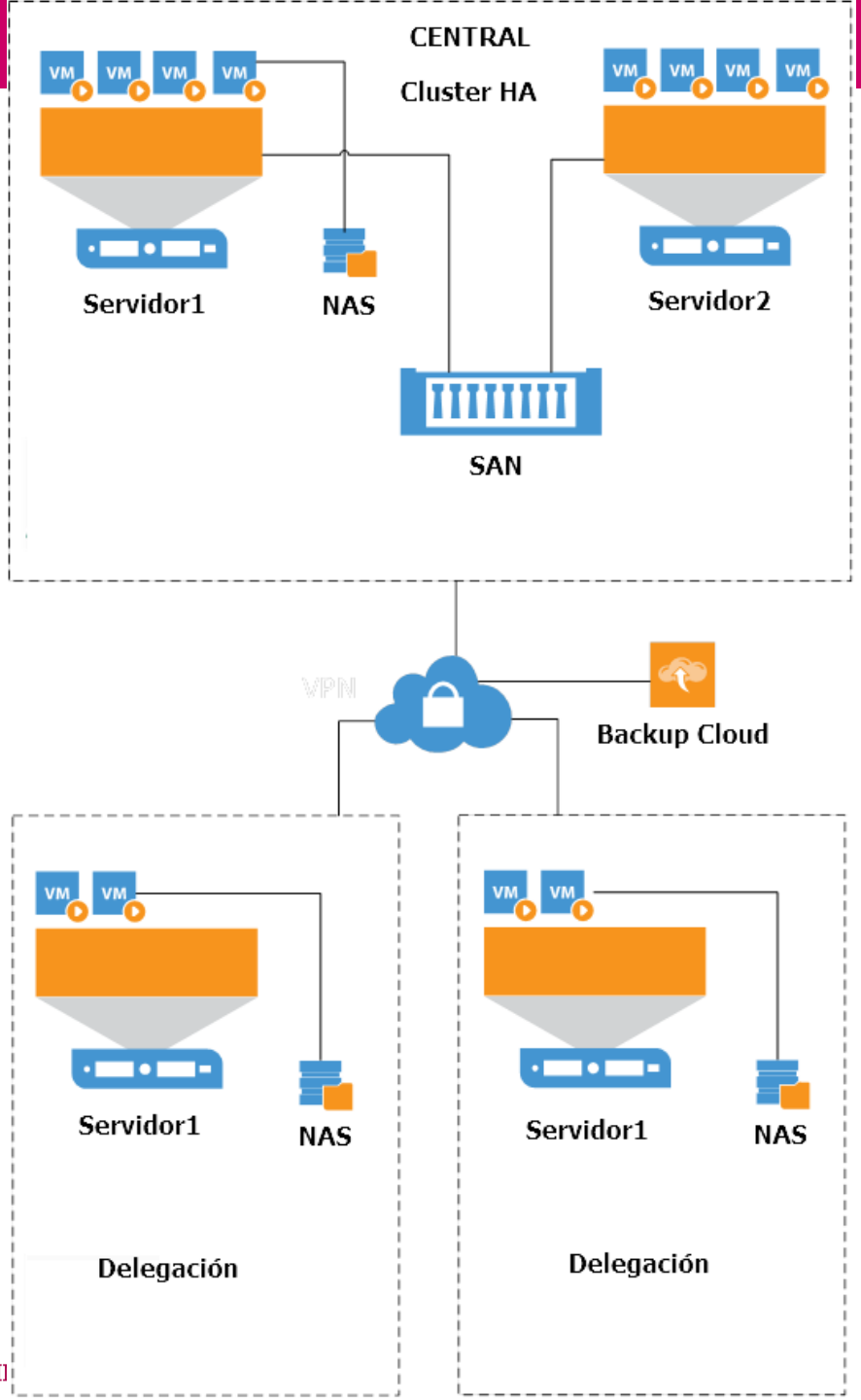
  PDS Plan Director de Seguridad

  Servicios Gestionados de Ciberseguridad. vCISO

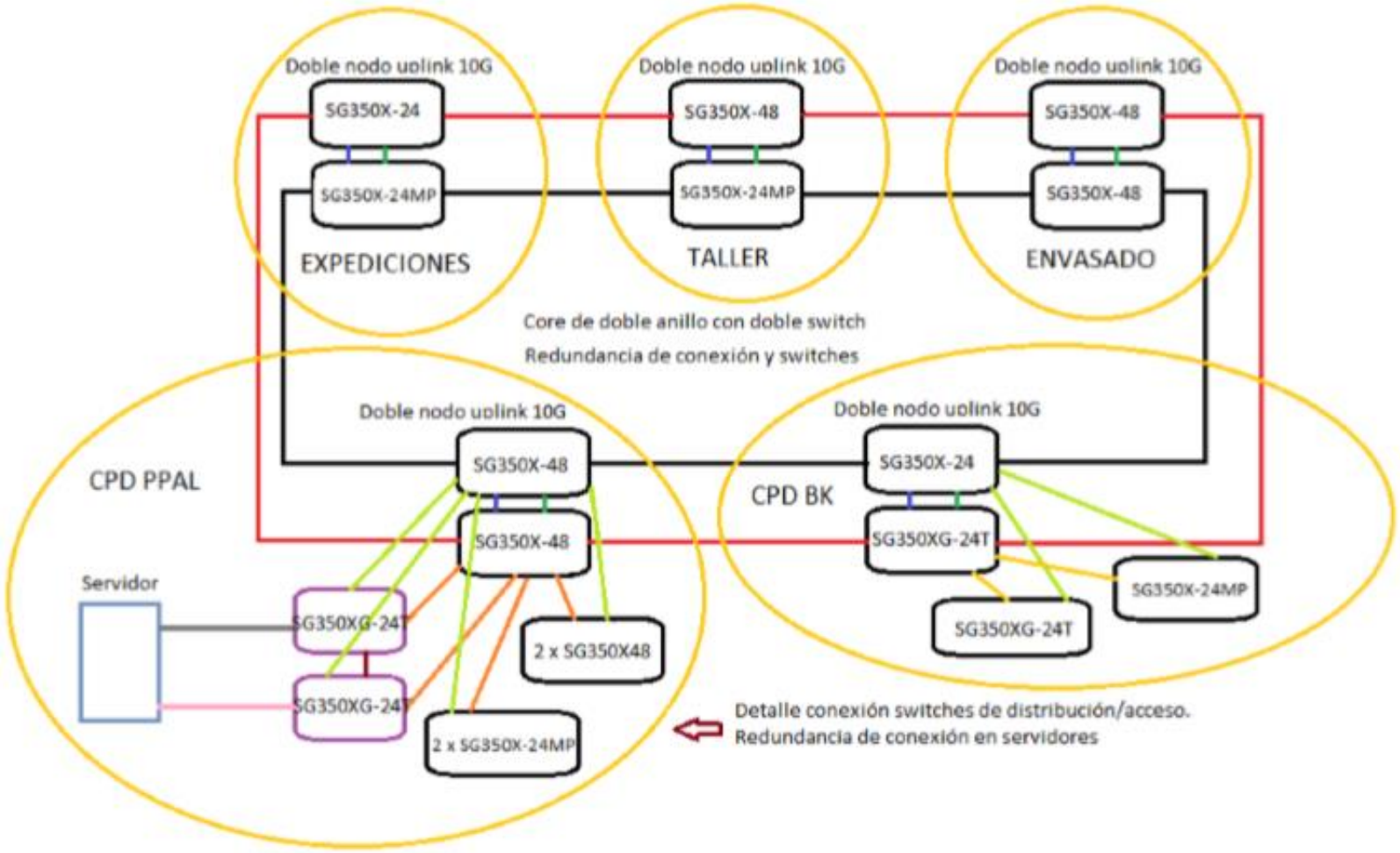
> **Formación y concienciación**
  - Formación y concienciación

Gestionar las TIC – Seguridad Física





Gestionar las TIC – Seguridad Física



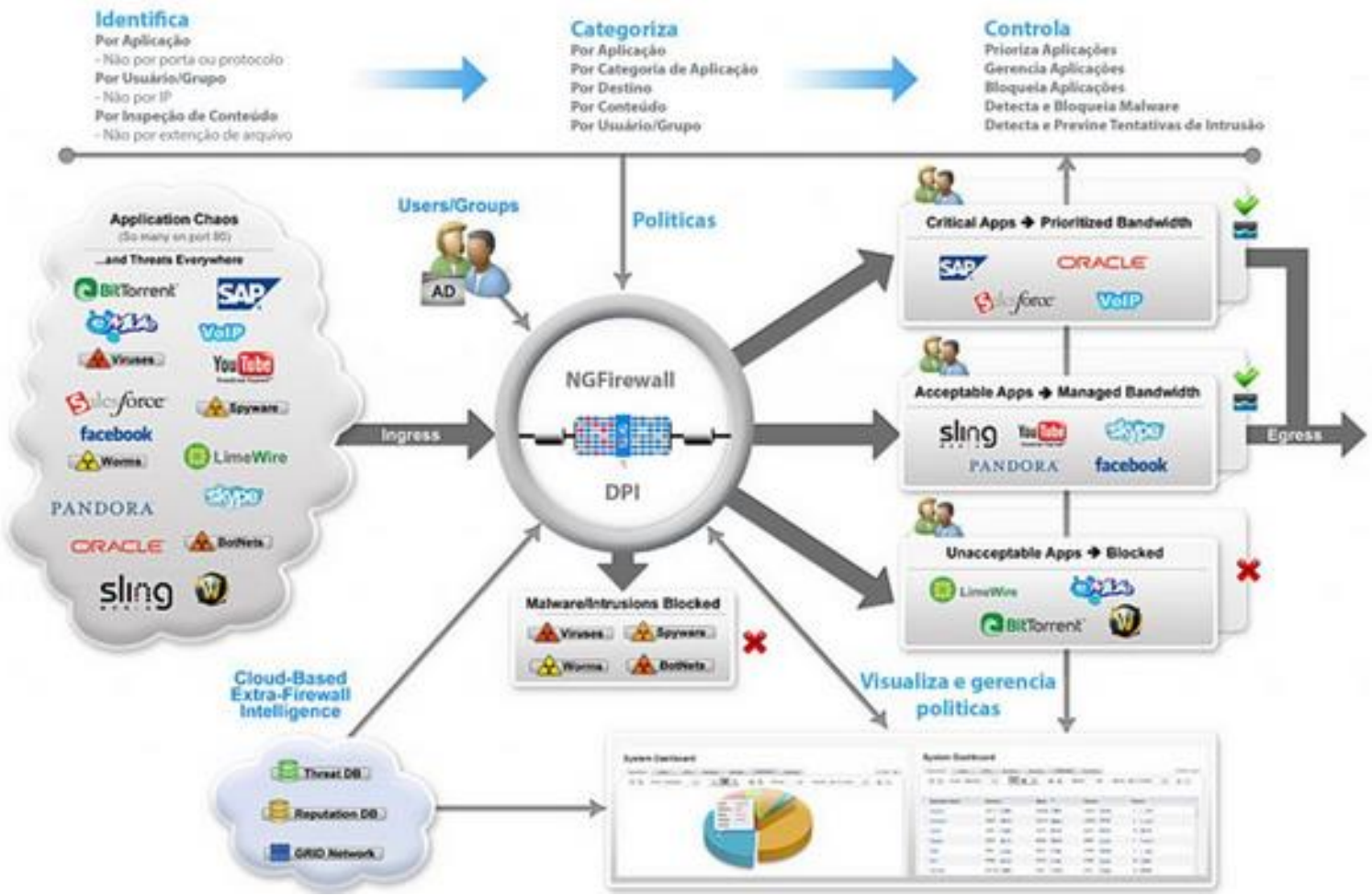
Gestionar las TIC – Seguridad Lógica

Seguridad en el perímetro

- Application Control
- Antivirus
- **Next Generation Firewall**
- Web Filtering
- AntiSpam
- WAN Acceleration
- Traffic Optimization
- VPN
- IPS
- DLP
- WiFi Controller

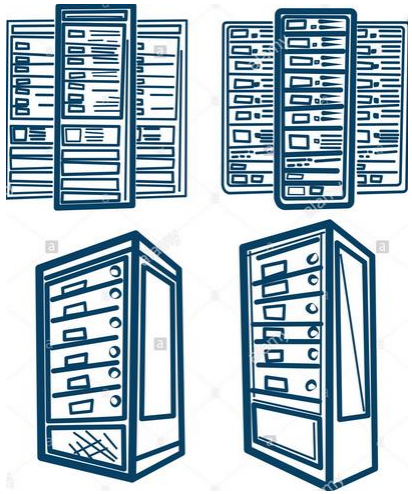
Gestionar las TIC – Seguridad Lógica

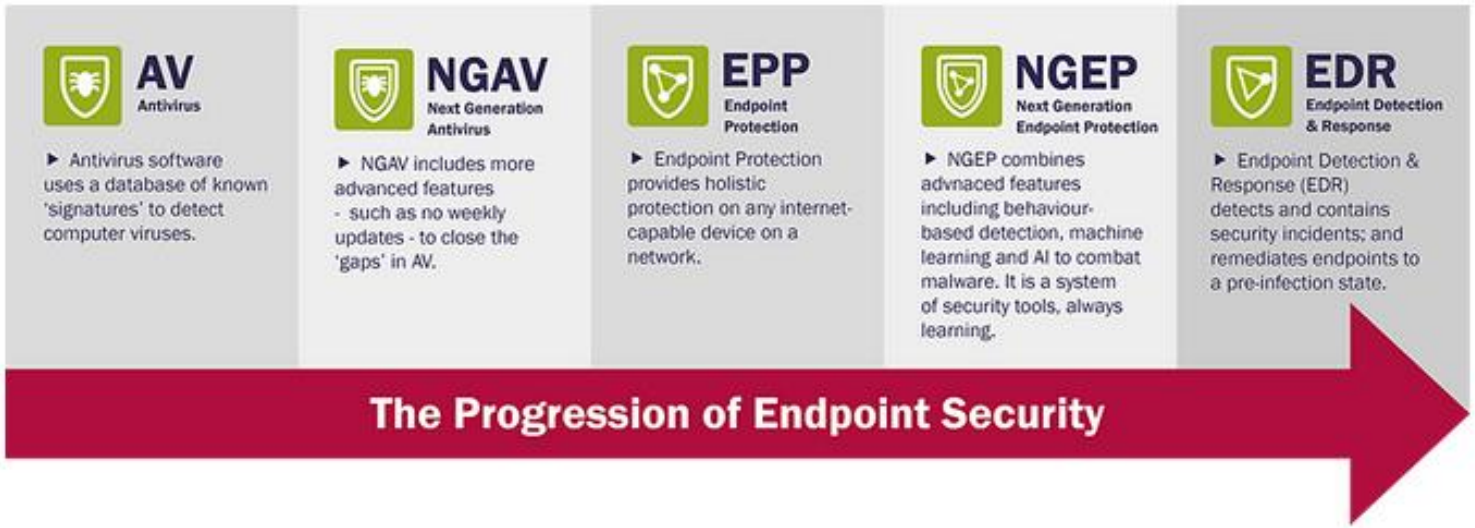
Seguridad en el perímetro



Gestionar las TIC – Seguridad Lógica

Seguridad en el host y servicios





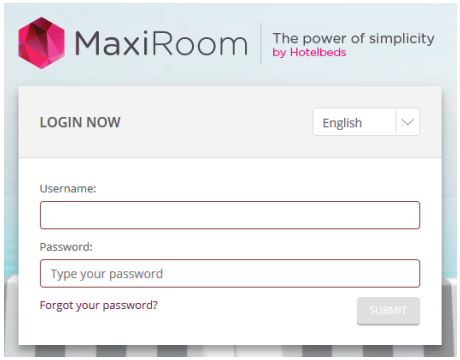
Gestionar las TIC – Seguridad Lógica

Seguridad del dato

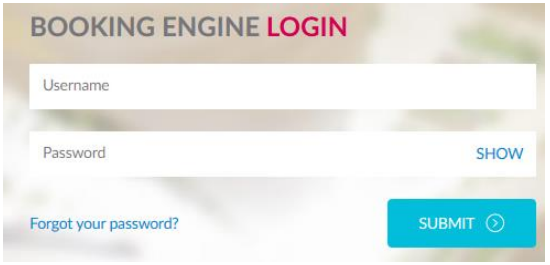
Cifrado

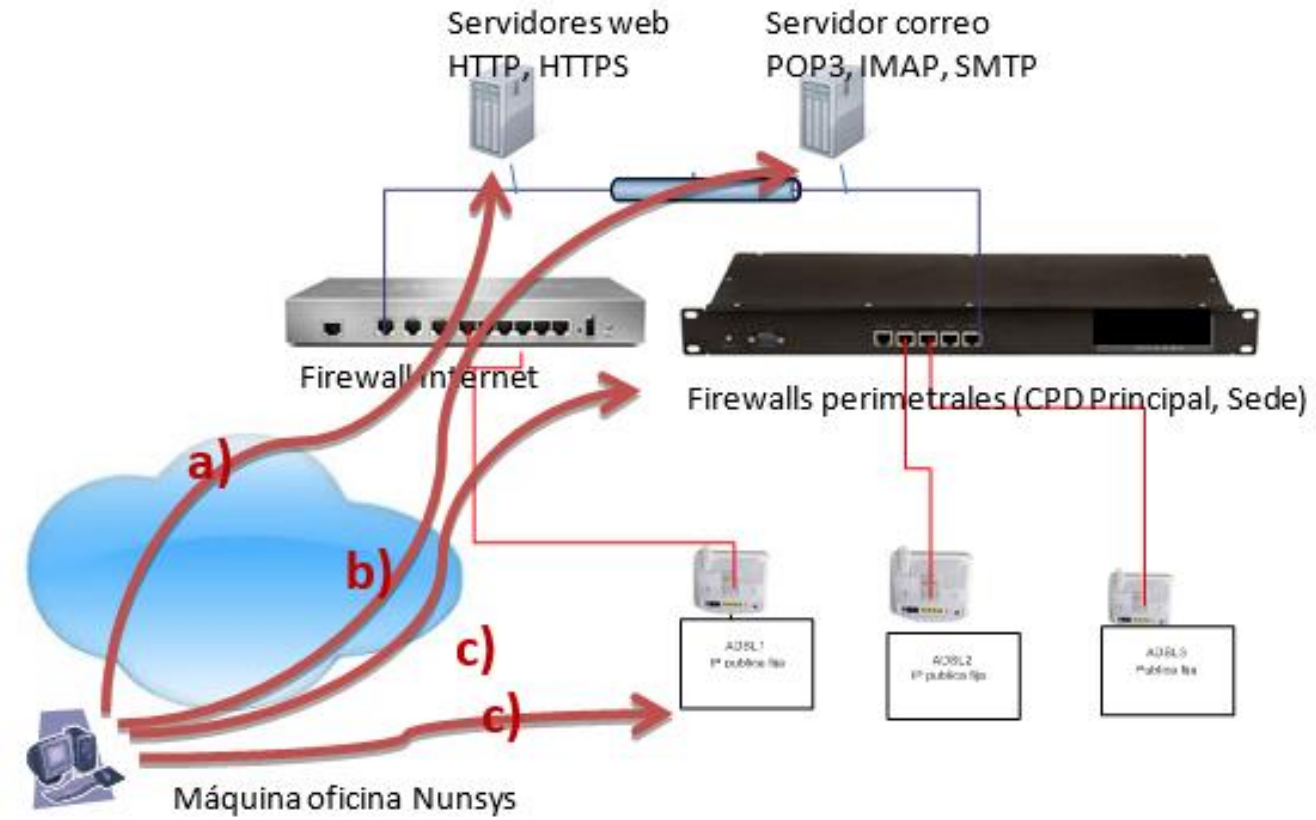
DLP

IRM



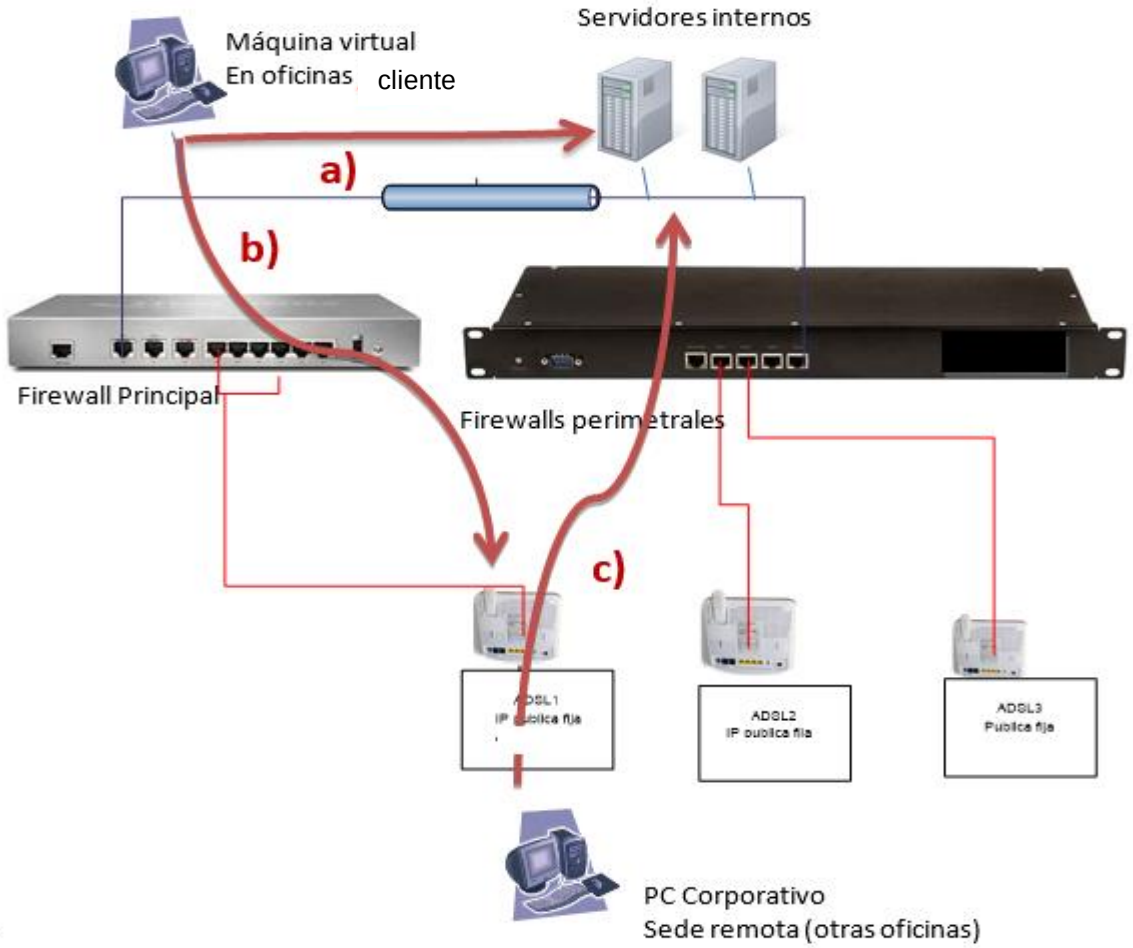
Auditoría de Seguridad Externa





Auditoría de Seguridad Interna

Acceso como proveedor
Acceso como empleado
Acceso como usuario



Fase 1 - Target discovery and Network Mapping

- *Escanear el objetivo para obtener información específica; información del entorno público , mapeo de la red y de los sistemas desde una pespectiva interna y externa. Recoger una gran fuente de información sobre el objetivo nos ayudará a planificar las pruebas a realizar.*

Fase 2 Vulnerability Scanning

- *Utilizando la información recogida en la Fase 1, se inicia el escaneo a nivel de red y de aplicación, y las entrevistas para detectar las vulnerabilidades sobre los controles de red, sistema y aplicación.*

Fase 3 – Exploitation

- *Se intenta superar los mecanismos de protección mediante la información obtenida en las fases anteriores.*

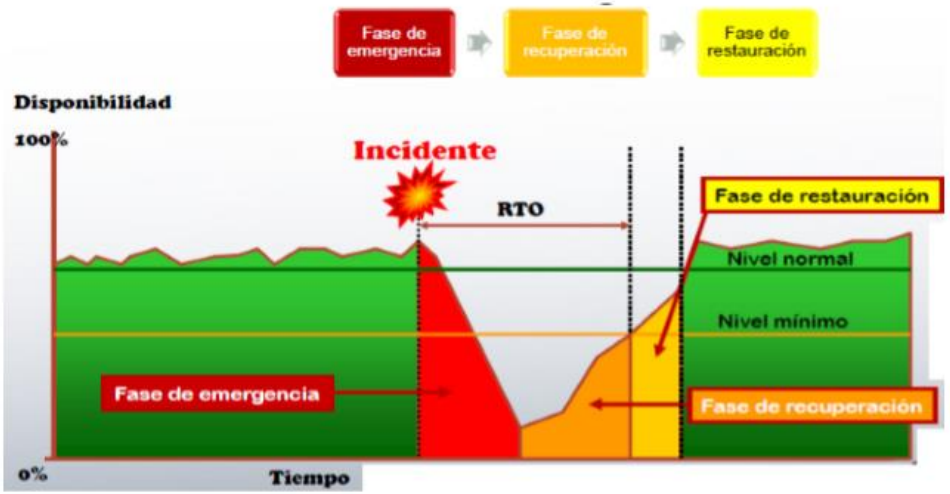
Fase 4 – Reporting

- *Desarrollar un informe con los resultados de la auditoría*

Plan de contingencia

• **¿Qué?:** Definir las partes de la organización que serán críticas en los primeros momentos y por tanto, que deberán volver a la normalidad lo antes posible.

• **¿Quién?:** Qué personas se tendrán que movilizar y en qué orden, cuanta gente hará falta en las primeras horas, los primeros días y sobre todo, cómo se coordinará el tema para que no se dé una situación caótica.



• **¿Dónde?:** A qué lugares tendremos que acudir para poder hacer todo esto. Si las ubicaciones físicas principales están afectadas, hay que tener lugares alternativos donde poder desplegar el Plan. ¿Qué pasa si no tengo mi equipo habitual o no se puede entrar al centro de proceso de datos (CPD) de la Organización?

• **¿Cómo?**: Aquello que tendremos que hacer para mitigar la contingencia, para entrar en la fase de recuperación y, por último, volver a la normalidad.

• **¿Cuándo?:** ¿Qué ventanas de interrupción son tolerables? ¿En cuánto tiempo tenemos que volver a la normalidad?

PDS Plan Director de seguridad

PDS Plan Director de seguridad

¿Por dónde empezar? Cuando decidimos abordar la ciberseguridad es importante tener una planificación de las actividades a realizar que cuente con el **compromiso de la dirección**.
Este plan va a marcar las prioridades, los responsables y los recursos que se van a emplear para mejorar nuestro nivel seguridad en el mundo digital.

Manos a la obra

La **participación de la dirección** será necesaria en los siguientes hitos:

- **Kick of del proyecto**
- **Reuniones iniciales** de identificación de servicios de la empresa, y valoración de las dimensiones de la seguridad: Integridad, disponibilidad, confidencialidad, trazabilidad, etc. del proceso de producción, y del negocio de la empresa. Identificar los riesgos más importantes que detecta dirección.
- **Mitad del proyecto**, resultado del análisis de riesgo, para definir estrategias de mitigación, presupuesto, capacidad de inversión, etc
- **Final del proyecto**, para presentar resultados del Plan Director de Seguridad

PDS Plan Director de seguridad

El proyecto debe comprender

- **Inventario de activos, análisis de riesgos y auditoría de buenas prácticas de seguridad** conforme al estándar internacional ISO 27002:2013 la cual incluye **114** controles de seguridad que serán analizados con el objetivo de elaborar el **Plan Director de Seguridad**.

- **Acompañamiento a la implementación:**
  Ejecutar proyectos "quick wins" de seguridad, resultantes del Plan Director de Seguridad

Se debe hacer especial hincapié en riesgos y controles a implantar en materia de ciberseguridad con vistas a la protección de la información

- Intercambio de información entre clientes, proveedores, …
- Información de proyectos
- Pérdida de información
- …

La prioridad de las tareas de resolución deberá quedar determinada por los riesgos a los que se encuentre expuesto y que hayan sido identificados en las etapas de **análisis de riesgos y auditoría de controles de la ISO 27002**.

PDS Plan Director de seguridad

Ejemplo de posibles quick wins a desarrollar**:**

- Desarrollar una **política de seguridad y normativas de seguridad** asociadas al uso del correo electrónico, dispositivos corporativos, etc.
- **Concienciación** a empleados de forma teórica y práctica para comprobar y aumentar el nivel existente en la empresa.
- **Controles** relacionados con la información: Clasificación, etiquetado, y control de la misma, dentro y fuera de la organización (Gestión de derechos en los documentos RMS, auditoría de acceso a carpetas y ficheros, etc.).
- Evaluación del proceso de **intercambio de información** con proveedores y clientes, cifrado, correo seguro y autenticado, integración con office 365. Posiblemente ya securizado, pero pendiente de incorporar a servicios gestionados.
- **Auditoría** de seguridad de sistemas y aplicaciones críticas
- **Control de acceso** físico, para controlar el acceso a zonas restringidas, y la identificación de personal de la empresa, terceros, y ajenos
- Implantación de una herramienta de prevención de fuga de información, **DLP**, y de control de dispositivos móviles (**MDM**).
- Implantación de buenas prácticas **ITIL**.
- Implantación de **Seguridad Gestionada**
- **Mejora** de la seguridad gestionada con nuevos elementos para el análisis
- …

PDS Plan Director de seguridad

Queremos Seguridad - ¿Tenemos claros los criterios, controles, procedimientos, …?

Introducción al plan

Abordar la ciberseguridad ➡ Planificación de las actividades ➡ Compromiso de Dirección

- Prioridades
- Responsables
- Recursos

PLAN DIRECTOR DE SEGURIDAD

- Proyectos técnicos
- Proyectos de contenido legal
- Proyectos organizativos

De este modo los proyectos podrán tratar …

- instalación de productos o de contratación de servicios
- cumplimiento con las leyes de privacidad y comercio electrónico
- formación de empleados
- puesta en marcha de procedimientos y políticas internas
- …

PDS Plan Director de seguridad

Requisito legal del Reglamento Europeo de Protección de datos (art. 30)

> El controlador y el encargado de tratar los datos deberán aplicar las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad acorde con los riesgos que presente el tratamiento, teniendo en cuenta los resultados de una evaluación de impacto sobre la protección de datos (con arreglo al Artículo 33), teniendo en cuenta la tecnología avanzada necesaria y el coste de su implementación.

Cada empresa … un mundo.

1. Calcular el actual nivel de seguridad (Punto de partida)
2. Fijar objetivo de dónde queremos estar.

Objetivo y proyectos a aplicar **SIEMPRE** alineados con la estrategia de negocio

- Qué vamos a proteger
- Cómo haremos la prevención
- Posibles incidentes a los que nos podemos enfrentar
- Preparación para cómo reaccionar
- …

Evaluación del riesgo que nos afecta y que podemos tolerar

Siempre midiendo el progreso

PDS Plan Director de seguridad

Inventariado de activos y Análisis de riesgos

ISO 27005

norma reconocida para la elaboración de un **Análisis de Riesgos** que nos conduzca a un correcto Plan Director de Seguridad

ISO27000

establece una implementación **efectiva** de la seguridad de la información empresarial

El Plan Director de Seguridad estará formado por:

1. Las medidas que garanticen la mitigación de los riesgos considerados relevantes
2. Proyectos tendentes a la mejora de la seguridad de la Organización

GDPR

Objetivos ➡ asegurar los pilares básicos de la seguridad:

- Disponibilidad
- Confidencialidad
- Integridad
- Autenticidad
- Trazabilidad

PDS Plan Director de seguridad

Cumplimiento de normativas

PDS Plan Director de seguridad

Cumplimiento de normativas

Derechos ARCO

ACCESO

Pedir al responsable de los ficheros, cómo está tratando tus datos

RECTIFICACIÓN

Para modificar cualquier dato erróneo

CANCELACIÓN

No poder usar los datos por exceso o por ser inapropiados

OPOSICIÓN

A que traten mis datos

PORTABILIDAD

Para que mis datos puedan ser transferidos a otro responsable

OLVIDO

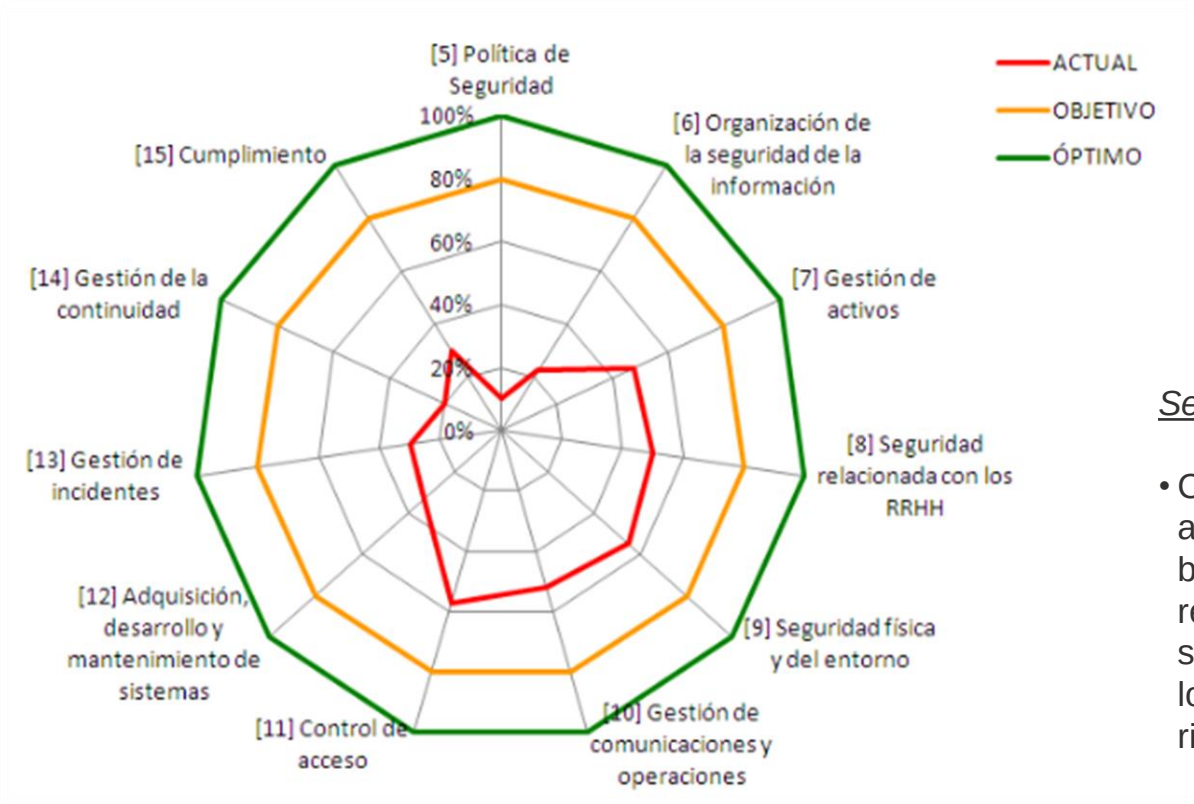
Solicitar que la información sea eliminada por completo

Sanciones graves (de 600 a 600.000 €)

Grabación en vía pública no debidamente notificada

PDS Plan Director de seguridad

Metodología



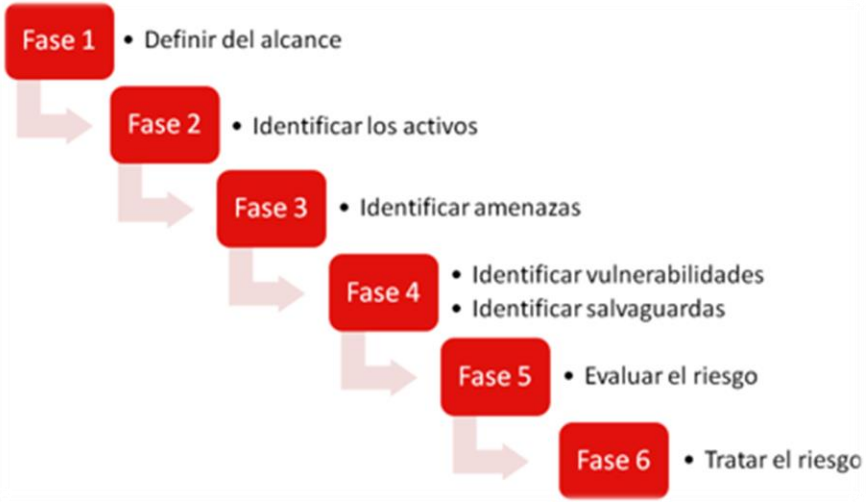
Selección de controles de seguridad

- Comprobación de medidas de seguridad actuales y su nivel de madurez según buenas prácticas (27002 y RGPD) que recogen los controles vinculados a la seguridad de la información, en base a los riesgos detectados en el análisis de riesgos.

- Comprobación y definición de las medidas previamente implantadas y la forma de afrontar las medidas que faltan por implantar o mejorar

PDS Plan Director de seguridad

Metodología



Análisis de riesgos

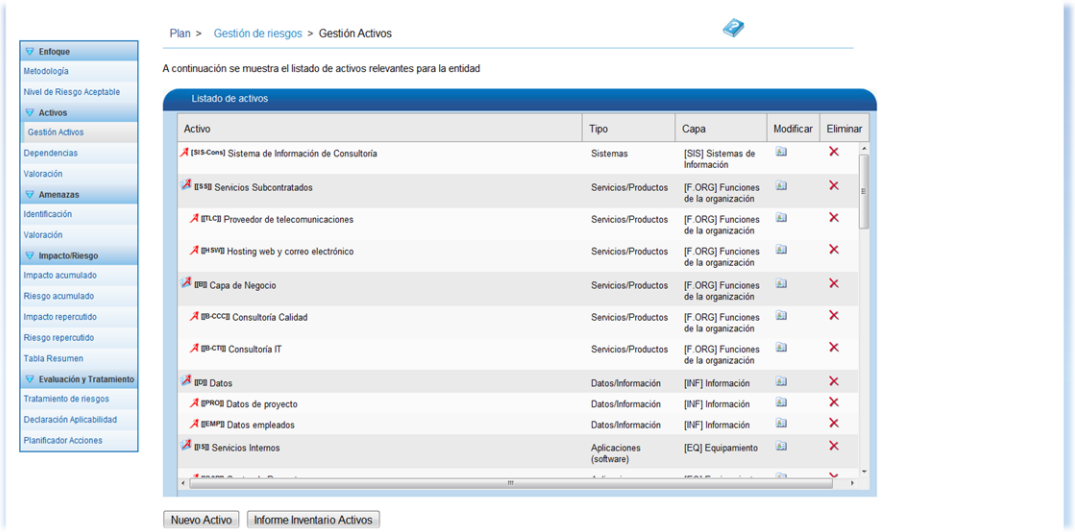
- Análisis mediante metodología MAGERIT y 27005 mediante herramienta GCONSULTING Compliance

Inventariado de activos

dependencia procesos negocio

Identificación de amenazas

Obtención de riesgos más críticos sobre los que se ven afectados los procesos de negocio implicados en el alcance del SGSI



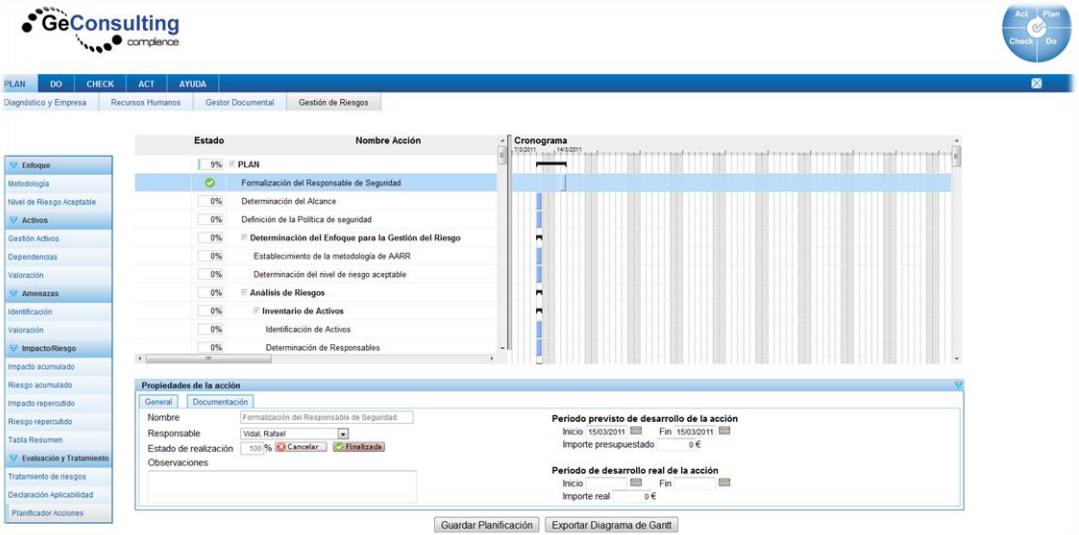
PDS Plan Director de seguridad

Metodología

Plan Director de Seguridad

- Detectados los riesgos
- Revisado el grado de implantación de los controles de la 27002 aplicables a los Sist. Inform.

- Redacción del plan de tratamiento de riesgos
- Proyectos estratégicos de implantación seguridad recogiendo medidas y controles para mejorar el nivel de madurez de la seguridad y el cumplimiento de las buenas prácticas



Se debe incluir en este apartado la revisión y redacción de la Política de seguridad a nivel corporativo, como punto de partida del Plan Director de Seguridad

PDS Plan Director de seguridad

Priorización de proyectos

- Priorización
  - Atendiendo a los resultados del Análisis de Riesgos priorizaremos las acciones, iniciativas y proyectos identificados.
- Clasificación
  - Atendiendo al esfuerzo y coste temporal: Acciones, Iniciativas y Proyectos
    - Corto
    - Medio
    - Largo

  - Además – Quick-Wins
    - Proyectos de menor esfuerzo y con una mejora sustancial en la seguridad
    - Se lanzan en cualquier momento
    - Objetivo: Obtener mejoras sustanciales en la seguridad del Plan Director de Seguridad

Etapas	1	2	3	4
Arranque del Proyecto				
Evaluación situación inicial				
Análisis de Riesgos				
Plan Director de Seguridad				
Comité de Seguridad				
Priorización de proyectos				
Implantación de Quick Wins				

Tu socio tecnológico

nunsys®

COMUNICACIONES · SISTEMAS · SOFTWARE · MARKETING · FORMACIÓN

economistas
Colegio de Valencia

La seguridad como Servicio Gestionado

Velando por la alineación entres las TIC y el objetivo de negocio

LA SEGURIDAD COMO SERVICIO GESTIONADO

Emmanuel Roesseler, Director de Sistemas de Seguridad de IBM España, Portugal, Grecia e Israel

Ante el fenómeno de Big Data, IBM aboga por poner en marcha un **sistema de seguridad integral** que unifique la seguridad de la información y la física, prevención de pérdidas y riesgos, e incluya soluciones que funcionen conjuntamente para proteger los activos de datos importantes.

A menudo, las empresas no orientan a los empleados sobre sus políticas de medios sociales en cuanto a seguridad. En primer lugar, hay que recordarles que no pueden revelar información confidencial.

http://www.redseguridad.com/especialidades-tic/amenazas-y-vulnerabilidades/la-evolucion-de-las-amenazas-en-internet-en-la-era-del-big-data

LOS 5 FRENTES DE LA SEGURIDAD

CIBERSEGURIDAD (Según Recomendación UIT–T X.1205: Unión internacional de Telecomunicaciones)

*"La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los **activos** de la organización y los usuarios en el ciberentorno"*

- Disponibilidad
- Confidencialidad
- Integridad
- Autenticidad
- Trazabilidad

LA SEGURIDAD COMO SERVICIO GESTIONADO

Disponibilidad

Implica que la información y los recursos relacionados estén siempre disponibles para el personal autorizado

"Garantizar la continuidad del negocio"

Confidencialidad

Evitar que personas no autorizadas puedan acceder a la información

"Proteger el acceso a la información"

Integridad

Garantizar que la totalidad de la información permanece inalterada

"Mantener la información completa y exacta"

Autenticidad

Asegurar que el origen (la propiedad) de la información es la original

"Velar por la suplantación de la identidad / propiedad"

Trazabilidad

Quién, cuándo, cómo, por dónde

"Poder seguir la traza de todo lo acontecido con la información"

PUNTOS BÁSICOS DE CUALQUIER EMPRESA

- PRODUCTIVIDAD / RENTABILIDAD
- CONTROL DE LA CALIDAD
- MEJORA CONTÍNUA

} **TIC → CIBERSEGURIDAD**

Disponibilidad

Implica que la información y los recursos relacionados estén siempre disponibles para el personal autorizado

"Garantizar la continuidad del negocio"

SINOPSIS
Un grupo terrorista bloquea el sistema de ordenadores que controla las comunicaciones, el transporte y el suministro de energía.

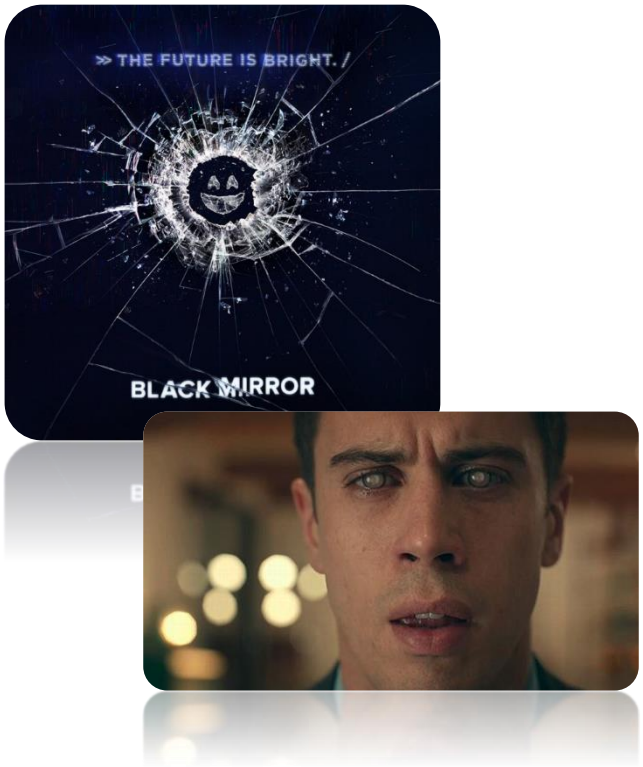
La disponibilidad es un factor clave para el desarrollo del negocio.

Que nunca se pare la cadena de producción

Confidencialidad

Evitar que personas no autorizadas puedan acceder a la información

“Proteger la información”



SINOPSIS "Tu historia completa“
Está situado en una realidad alternativa donde la mayoría de la gente tiene un "chip" implantado detrás de la oreja, que registra todo lo que hacen, ven o escuchan. Esto permite que los recuerdos puedan reproducirse ya sea delante de los ojos de la persona o en una pantalla, un proceso conocido como "revisar".

Que los planes estratégicos, proyectos de I+D+i, presupuestos, datos de clientes, … solo sean accesibles por el personal autorizado.

Integridad

Garantizar que la totalidad de la información se almacena y su contenido permanece inalterado

"Mantener la información completa y exacta"

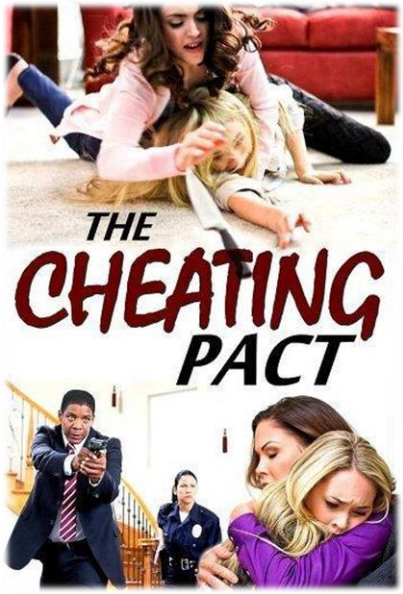
SINOPSIS
La memoria de Leonard, un investigador de una agencia de seguros, está irreversiblemente dañada debido a un golpe sufrido en la cabeza, cuando intentaba evitar el asesinato de su mujer: éste es el último hecho que recuerda del pasado. La memoria reciente la ha perdido: los hechos cotidianos desaparecen de su mente en unos minutos. Así pues, para investigar y vengar el asesinato de su esposa tiene que recurrir a la ayuda de una cámara instantánea y a las notas tatuadas en su cuerpo.

Hay que producir con un nivel de calidad y para ello el dato no se debe alterar por ningún agente externo al de la cadena de producción

Autenticidad

Asegurar que el origen (la propiedad) de la información es la original

"Velar por la suplantación de la identidad / propiedad"



SINOPSIS
Heather le pide a la alumna más aventajada de la clase que se haga pasar por ella en el examen de ingreso en la universidad a cambio de dinero. La joven acepta porque su familia lo necesita.

Los ejemplos más claros actuales son los de phishing en el email

Trazabilidad

Quién, cuándo, cómo, por dónde

"Poder seguir la traza de todo lo acontecido con la información"

SINOPSIS
Inspirada en los hechos que tuvieron lugar durante un intento por alcanzar el pico más alto del mundo, narra las peripecias de dos expediciones que se enfrentan a la peor tormenta de nieve conocida. En un desesperado esfuerzo por sobrevivir, el temple de los alpinistas se ve puesto a prueba al tener que enfrentarse a la furia desatada de los elementos y a obstáculos casi insuperables.

Para la ciberseguridad es vital tener **visión** de todo lo que acontece

SERVICIO GESTIONADO

Modelo de Servicios Gestionados (MSP)

Gestión y monitorización Pro-Activa

Mejora Continua

Dedicación de recursos TI especializados

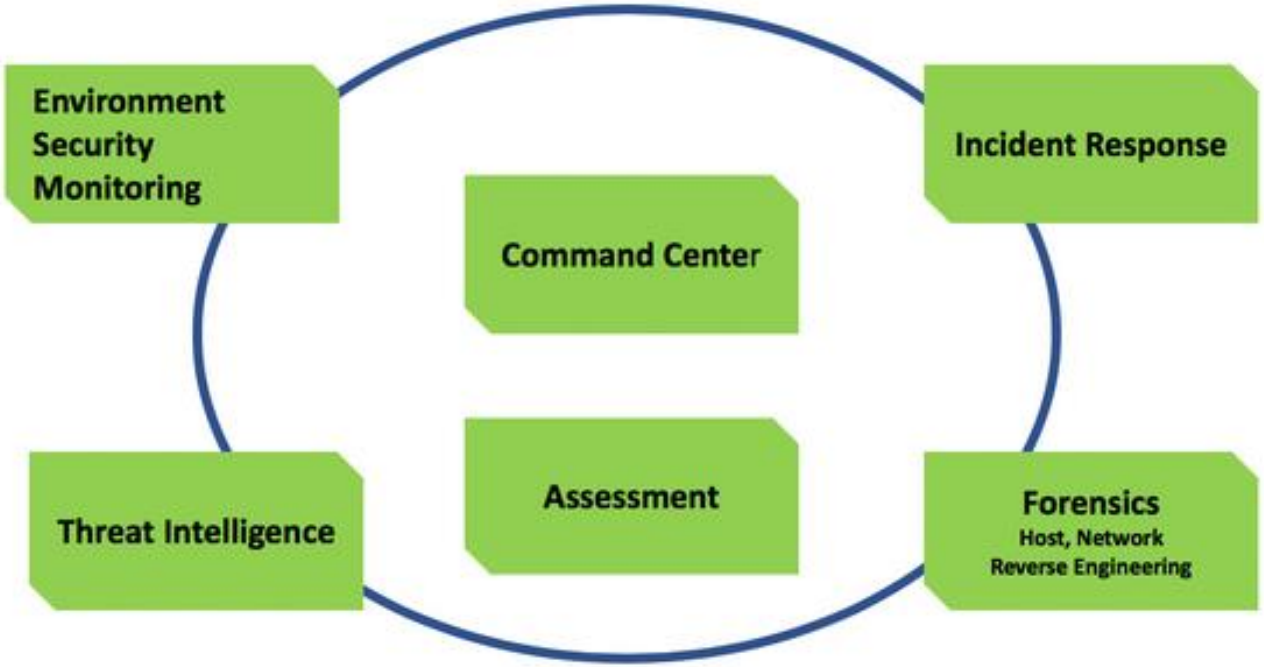
Minimizar Downtime y Maximizar Productividad

Informar y asesorar

Gestión del Servicio basado en ITIL

- Proporcionar servicios fiables y consistentes
- Capacidad para formalizar y medir niveles de servicio.
- Uso eficiente de recursos y personas.
- Servicios capaces de controlar, evaluar y absorber cambios con interrupción nula o mínima.
- Disminución de costes y riesgos.
- Incremento de la productividad y competitividad del negocio.

CSOC
CYBERDEFENCE SECURITY OPERATION CENTER



CICLO CONTINUO






Detectar

- Deteccion de ataques
- Escaneo vulnerabilidades
- Red de Vigilancia
- Detección de anomalías
- Firewall
- Cacheo eventos

Recoger y Almacenar

- Evento recolección
- Filtrado de eventos
- Almacenamiento SQL
- Archivo Forense
- Firma Digital
- Comunicaciones Seguras y Fiables.
- 5 GBs Throughput
- Packet capture

Correlacionar

- Correlación Lógica
- Correlación Cruzada
- Correlación Inventario
- Situational awareness
- Taxonomia de eventos

Informe

- Dashboard & Métrica
- Informes de Seguridad
- Informes vulnerabilidades
- Informes de Disponibilidad
- Informes de Red
- Informes Forenses
- Informe Ejecutivo
- Generador Informes
- Modulos predefinidos
- Personalizables
- Planificador

Administrar

- Evaluación de Riesgos
- Apoyan la Decisión
- Respuestas Automáticas
- Gestión de Incidencias
- Gestión de Inventario
- Mgmt Jerárrquico
- MultiCliente
- Gestión Centralizada
- Distribución
- Escalabilidad
- HA & Equlibrio de Carga

Conformidad

- Personalización de paneles ejecutivos.
- Métrica

PERSONAL CERTIFICADO

- APEP Certified Privacy – Asociación Profesional Española de Privacidad
- ISO 27001 Lead Auditor
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA).

LA SEGURIDAD COMO SERVICIO GESTIONADO

Gestión de la capacidad y disponibilidad:

Mediante monitorización, basada en una administración activa de los servicios relacionados con el Sistema de Información, proporcionando una supervisión continua de los sistemas y componentes (24x7x365) desde una localización adecuada al servicio ofertado y equipada con tecnologías de última generación.

Las incidencias o posibles inestabilidades en los equipamientos son detectadas de forma inmediata, permitiendo una rápida resolución de las mismas, evitando pérdida de tiempo y productividad, y en consecuencia; pérdidas financieras.

Análisis de comportamiento:

Se trata del análisis pormenorizado del tráfico de red, en busca de ataques conocidos, o comportamientos sospechosos, como puede ser el escaneo de puertos, paquetes malformados, etc. con el objetivo de detectar y/o prevenir intrusiones en el Sistema de Información (24x7x365).

A través de soluciones de IDS/IPS, no sólo analiza qué tipo de tráfico se genera, sino que revisa contenido y su comportamiento.

De este modo puede contar con un servicio de notificación de alerta temprana de riesgos, amenazas o incidentes que puedan afectar a los Sistemas de Información.

LA SEGURIDAD COMO SERVICIO GESTIONADO

Gestión de vulnerabilidades:

Continúa supervisión, seguimiento y mejora de la seguridad de su Sistema de Información (red, aplicaciones, infraestructura, etc.), ejecutando periódicamente escaneos con el objetivo de identificar, cuantificar y clasificar las vulnerabilidades de su Sistema.

Analizado el riesgo que supone cada vulnerabilidad encontrada para la organización se desarrollan las medidas de mitigación oportunas.

Esto supone el acceso a servicios de carácter preventivo orientados a proteger de una manera más eficiente los Sistemas de Información.

Respuesta a Ciberincidentes:

Junto a los servicios de Gestión de la capacidad y disponibilidad y/o Análisis de comportamiento se ofrece, una vez detectada la incidencia, fallo, avería u origen de la degradación del nivel de Servicio en los componentes que forman el Sistema de Información monitorizado, desarrollar las acciones correctivas adecuadas.

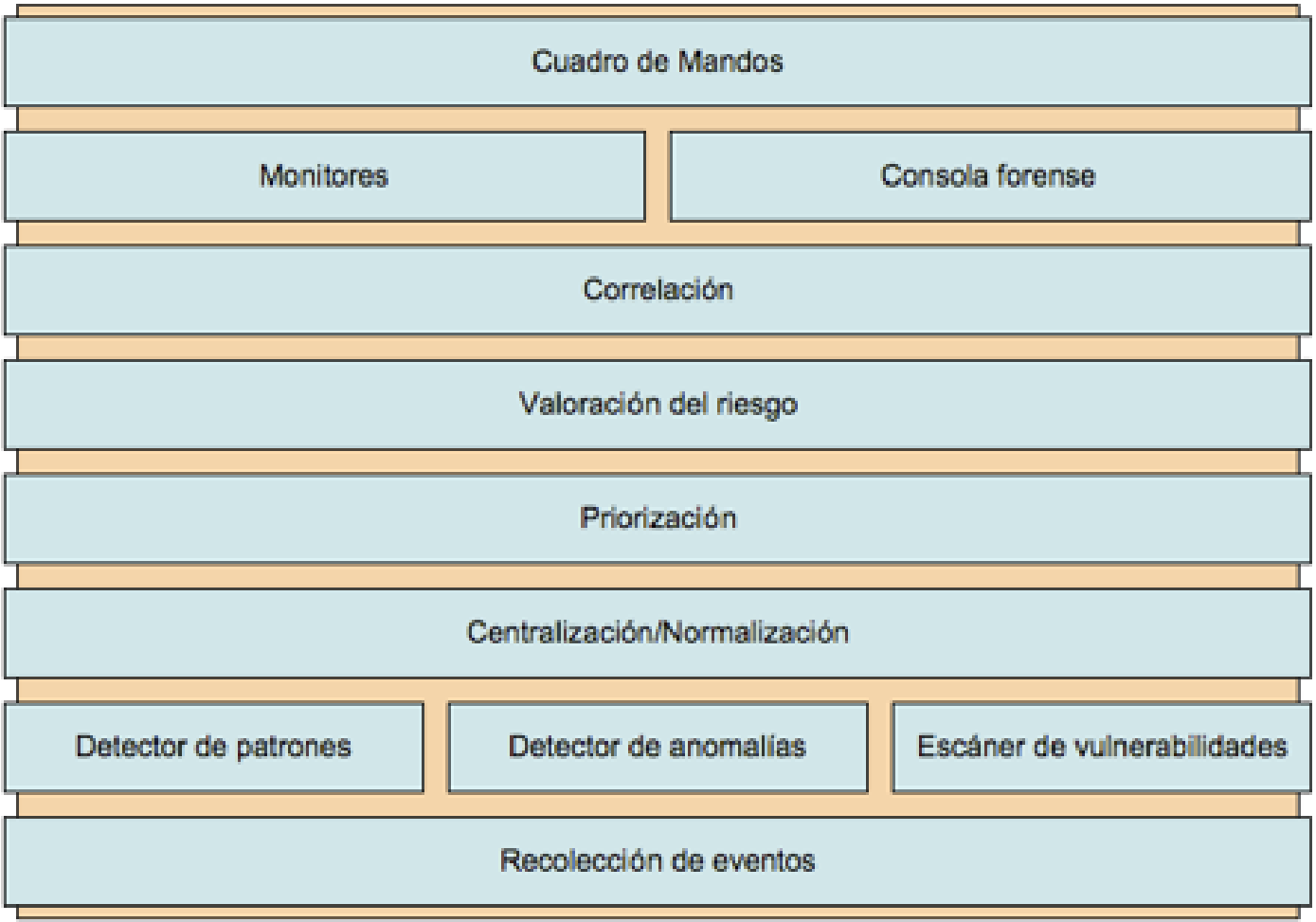
Para ello nunsys pone a disposición un equipo técnico especializado (24x7x365) en la gestión de ciberincidentes con el objetivo de aumentar la capacidad de mitigación del incidente a través de la coordinación con los diferentes agentes implicados, como proveedores de servicios en internet u otros proveedores dentro de la cadena de suministro del servicio.

Virtual Chief Information Security Officer (vCISO):

El CISO es un rol desempeñado a nivel ejecutivo y su función principal es la de alinear la seguridad de la información con los objetivos de negocio. De esta forma se garantiza en todo momento que la información de la empresa está protegida adecuadamente. El equipo de Consultores de nunsys asume las siguientes responsabilidades:

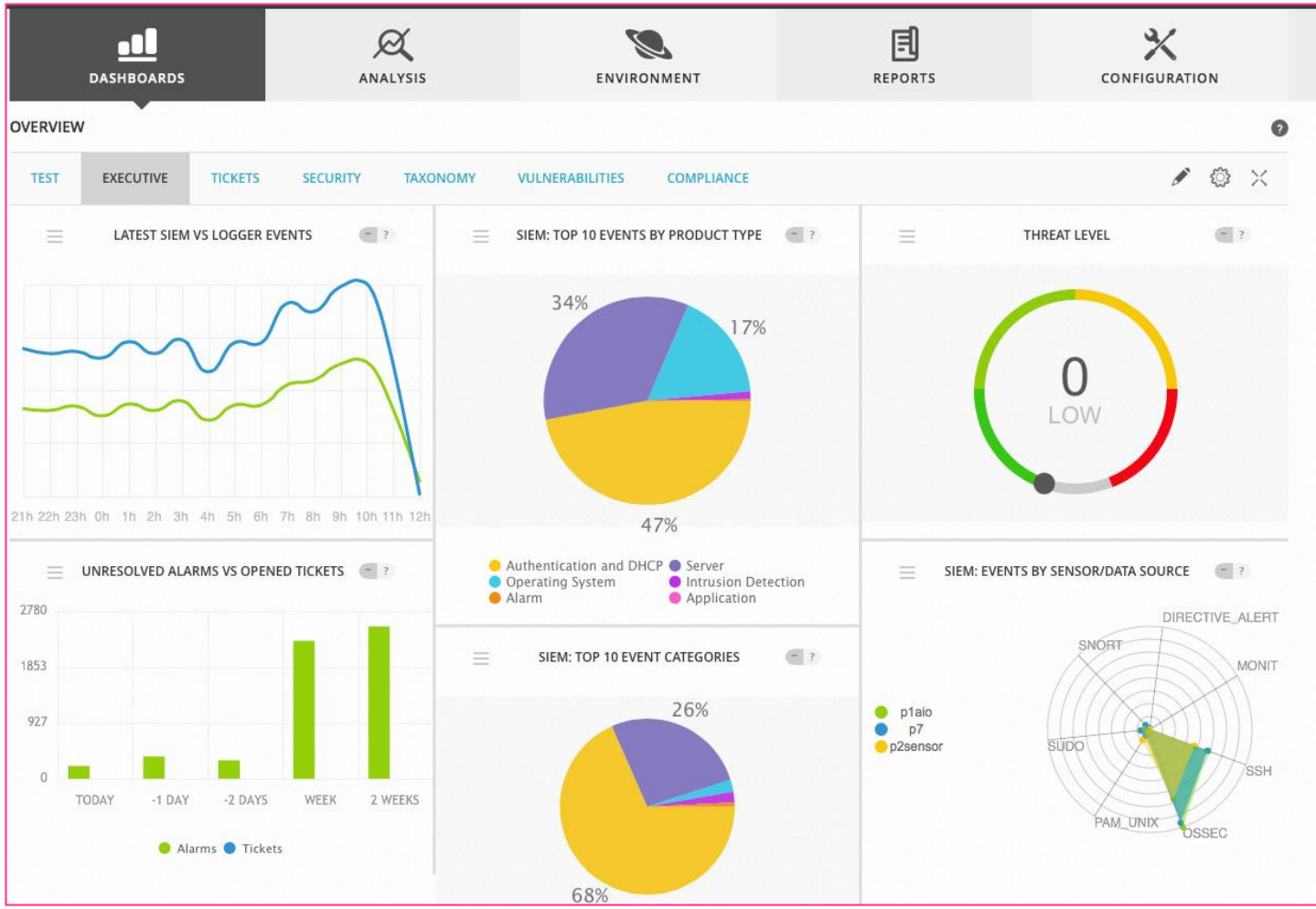
- Generar e implantar políticas de seguridad de la información.
- Mejorar reglas de detección / correlación / protocolos de actuación.
- Supervisar la administración del control de acceso a la información.
- Supervisar el cumplimiento normativo de la seguridad de la información.
- Responsable del equipo de respuesta ante incidentes de seguridad de la información de la organización.
- Supervisar la arquitectura de seguridad de la información de la empresa.
- Mejoras en Gestión y configuración de Seguridad (Redes y Sistemas)
- Análisis de informes mensual y asesoramiento

Arquitectura de 8 capas

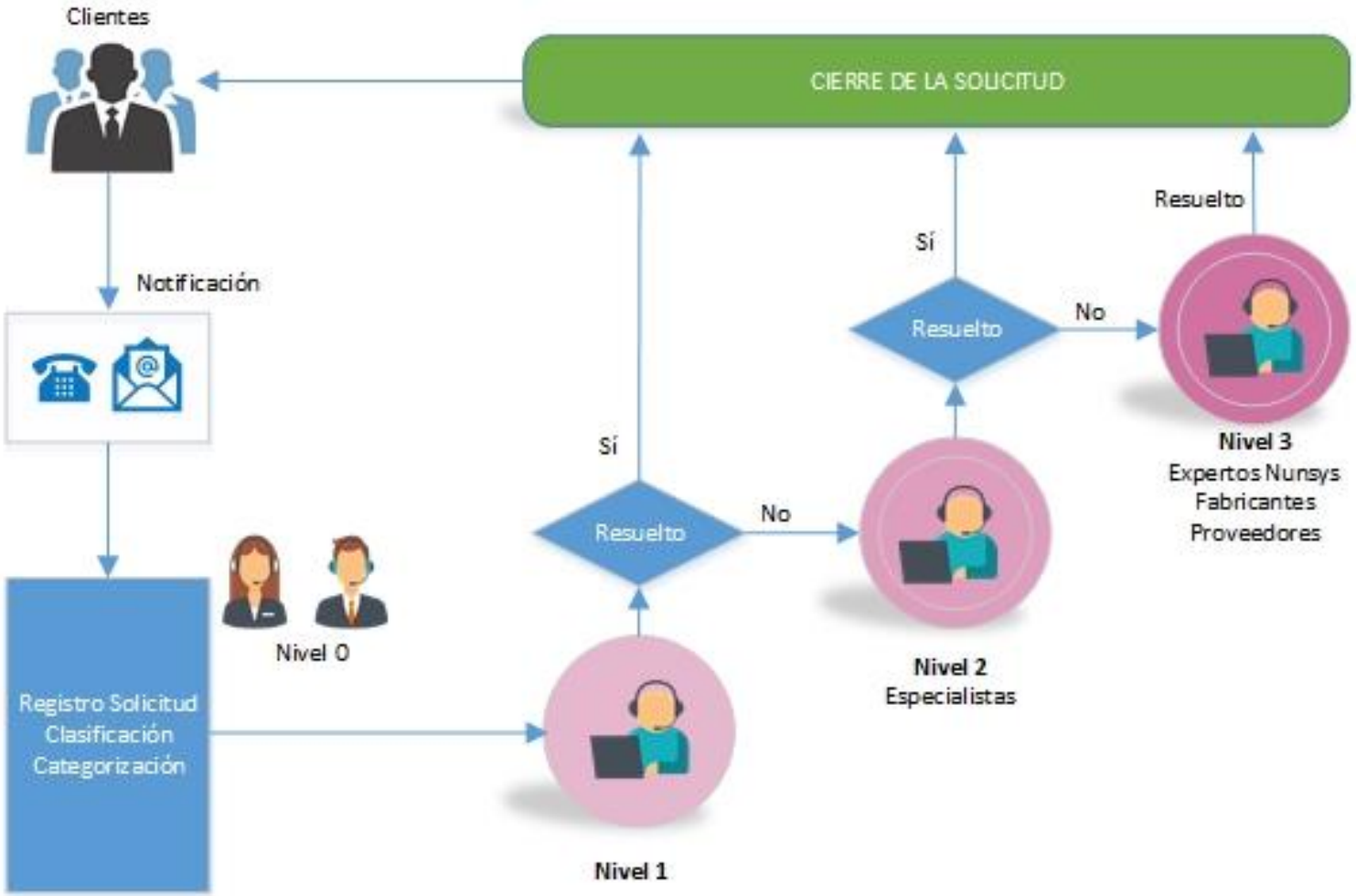


Cuadro de mandos

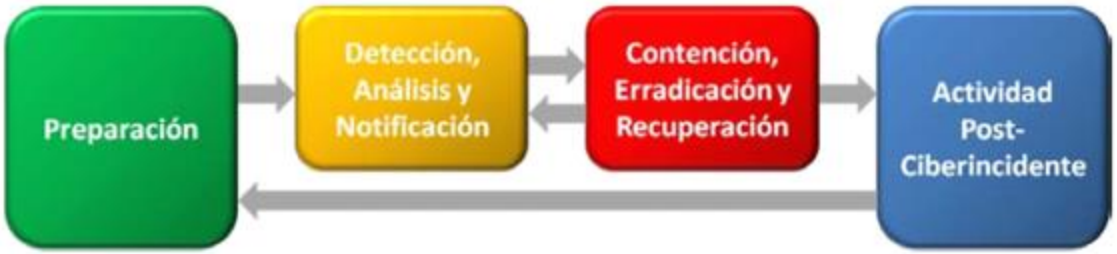
- Cuadro de mandos Personalizable
- Estado de la seguridad y disponibilidad
- Umbrales y objetivos a cumplir
- Información concisa y simple
- Termómetro de la red



SAT – Servicio de Asistencia Técnica



GESTIÓN DE INCIDENCIAS



Ciclo de vida de la Respuesta a Ciberincidentes

Los objetivos del plan son:

1. Asegurarse de que el incidente sí se ha producido en la entidad (descartar falsos positivos)
2. Mitigar el impacto del incidente.
3. Encontrar la forma como el atacante ha provocado el incidente de la entidad.
4. Prevenir futuros ataques o incidentes.
5. Mejorar la seguridad y respuesta a incidentes.
6. Mantenerse informado de la gestión de la situación y la respuesta a la entidad.

PRIORIDAD y SLA

PRIORIDAD		IMPACTO		
		Organización	Departamento o Grupo	Usuario
URGENCIA	Alta	Alta	Alta	Media
	Media	Alta	Media	Baja
	Baja	Media	Baja	Baja

PRIORIDAD	TIEMPO DE RESPUESTA
Alta	1 hora
Media	2 horas
Baja	4 horas

Tu socio tecnológico

nunsys®

COMUNICACIONES · SISTEMAS · SOFTWARE · MARKETING · FORMACIÓN

economistas
Colegio de Valencia

Formación y Concienciación

La base de una correcta implementación

EJECUCIÓN DE UN PROYECTO DE CONCIENCIACIÓN

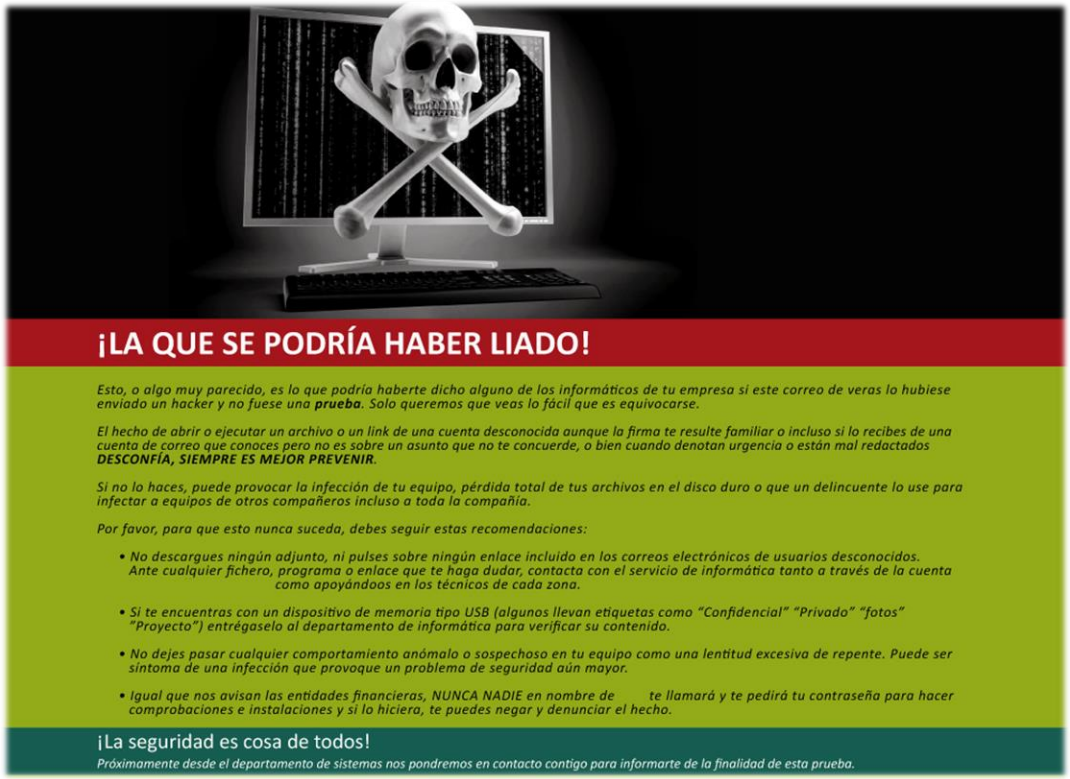
F0. Arranque del proyecto y planificación de ejecución.	• Planificación
F1. Desarrollo sesión de concienciación a medida para CLIENTE	• Desarrollo de sesión a medida
F2. Desarrollo del contenido de los dos ataques dirigidos	• Correo personalizado y etiquetado de USB
F3 Jornadas presenciales de Concienciación.	• Impartición de Jornada por personal especializado.
F4 Distribución de ataques dirigidos.	• Spear phising & USB malware
F5. Informe de resultados	• Resumen del plan de concienciación

3 FASES

TEÓRICA
- Uso del correo electrónico
- Navegación Segura
- Redes Sociales
- Protección de Archivos
- Seguridad en Dispositivos USB
- Dispositivos Móviles
- Protección y destrucción de datos
- Seguridad en viajes

NORMATIVA
- RGPD
- ENS
- LEY PIC

PRÁCTICA
- USB / MAILIN
- HACKER



BIBLIOGRAFÍA / FUENTES

https://www.incibe.es/
https://ccn-cert.cni.es/
https://www.ticbeat.com/educacion/branded-utad-75-000-euros-coste-ciberataque-empresas/
https://www.directivosyempresas.com/empresas/impacto-economico-de-cibertataques/
https://ipmark.com/google-elimino-588-millones-anuncios-phising/
https://enterprise.verizon.com/resources/reports/dbir/
https://cybersecuritynews.es/el-coste-de-los-ataques-ciberneticos-han-aumentado-en-un-52/
https://criptomoneda.ninja/aplicaciones-blockchain/
https://www.akamai.com/es/es/resources/our-thinking/state-of-the-internet-report/web-attack-visualization.jsp
https://www.directivosyempresas.com/empresas/impacto-economico-de-cibertataques/

nunsys
Tu socio tecnológico

¡GRACIAS!

Enrique Rodríguez Lázaro
enrique.rodriguez@nunsys.com