

# CETIC (Centro de Tecnologías de la Información y Comunicación)



CETIC (Centro de Tecnologías de la Información y la Comunicación) ofrece un conjunto de recursos y actividades orientados a fomentar la capacitación profesional, el reciclaje y la inserción laboral a través de la realización de acciones de formación, orientación e información y el contacto con las empresas dentro del sector TIC.

## Contacto

- [C/ Castro Urdiales, 10](#)
- Tfno: 945 16 15 05 / Fax: 945 16 15 04
- [formacionempleo@vitoria-gasteiz.org](mailto:formacionempleo@vitoria-gasteiz.org)

# Cyber-Sec... Conceptos:

- **Seguridad de la Información:**
  - Conjunto de medidas (preventivas y reactivas) de las organizaciones y de los sistemas TI que permiten resguardar y proteger la información (*activos en papel y digital*), buscando la confidencialidad, disponibilidad e integridad de la misma.
- **Seguridad informática (CYBER SECURITY):**
  - Es la protección de los *activos digitales* (información, hardware y redes) frente a las amenazas en su procesamiento, almacenamiento y transporte por los sistemas interconectados.

# Cyber-Sec... Funciones:

- Identificar:
  - Minimizar el riesgo para sistemas, activos, datos y capacidades.
- Proteger:
  - Diseño de salvaguardas para limitar el impacto de eventos potenciales sobre servicios e infraestructuras críticas.
- Detectar:
  - Implementación de actividades para identificar ocurrencia de eventos de seguridad.
- Responder:
  - Toma de medidas adecuadas.
- Recuperar:
  - Planificado de la reparación de capacidades y servicios comprometidos.

FUNCTION UNIQUE IDENTIFIER	FUNCTION	CATEGORY UNIQUE IDENTIFIER	CATEGORY
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GB	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR_AC	Access Control
		PR_AT	Awareness & Training
		PR_DS	Data Security
		PR_IP	Information Protection Processes & Procedures
DE	Detect	DE_AE	Anomalies & Events
		DE_CM	Security Continuous Monitoring
		DE_DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Migration
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

## Cyber-Sec... Entidades:

- NIST <https://www.nist.gov/>
- ENISA <https://www.enisa.europa.eu>
  - <https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material>



Search NIST



[TOPICS](#)   [PUBLICATIONS](#)   [LABS & MAJOR PROGRAMS](#)   [SERVICES & RESOURCES](#)   [NEWS & EVENTS](#)   [ABOUT NIST](#)

**NOTICE: Due to a lapse in federal funding,  
most of this website is not available.**

[Learn More](#)

**Contract  
Performance  
and a Lapse in  
Appropriations**

[View document](#)

**Grantee  
Performance  
and a Lapse in  
Appropriations**

[View document](#)

NOTICE: Due to a lapse in federal funding, most of this website is not available.<sup>(\*)</sup>

Contract Performance and a Lapse In  
Appropriations

Grantee Performance and a Lapse In  
Appropriations

## MEASURE. INNOVATE. LEAD.

Working with industry and science to advance innovation and improve quality of life.



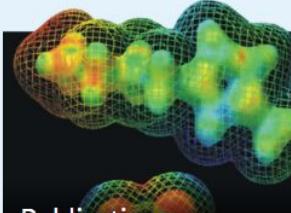
### Services & Resources

- [Calibrations](#)
- [Data](#)
- [Standards & Measurements](#)
- [Official U.S. Time](#)
- [Technology Partnerships](#)



### Labs & Major Programs

- [Laboratories](#)
- [User Facilities](#)
- [Baldrige Performance Excellence Program](#)
- [Manufacturing Extension Partnership \(MEP\)](#)
- [Industry Impacts](#)



### Publications

- [Weights and Measures Handbooks](#)
- [Baldrige Excellence Framework and Criteria](#)
- [Computer Security Publications](#)
- [Journal of Research of NIST](#)



Search NIST

NIST MENU

## Information Technology

### CYBERSECURITY

*NIST implements practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the U.S. to adopt cybersecurity capabilities.*

Computer Security Resource Center

Cybersecurity Framework

National Cybersecurity Center of Excellence

National Initiative for Cybersecurity Education (NICE)

Privacy Framework



NIST Releases Version 1.1 of its Popular Cybersecurity Framework



NIST Impacts: Cybersecurity

#### CYBERSECURITY TOPICS

Configuration & vulnerability management

Cryptography

Cybersecurity education & workforce development

Identity & access management

Risk management

With a world-class measurement and testing laboratory encompassing a wide range of areas of computer science, mathematics, statistics, and systems engineering, NIST's cybersecurity program supports its overall mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and related technology through research and development in ways that enhance economic security and improve our quality of life.

The need for cybersecurity standards and best practices that address interoperability, usability and privacy continues to be critical for the nation. NIST's cybersecurity programs seek to enable greater development and application of practical, innovative security technologies and methodologies that enhance the country's ability to address current and future computer and information security challenges.

#### NEWS AND UPDATES

##### **32nd Annual FISSEA Conference: Call for Presentations**

MARCH 27, 2019 TO MARCH 28, 2019

Call for Presentations The FISSEA Technical Working Group is seeking timely, topical, and thought-provoking...



## ENISA Topics

- [Cloud and Big Data](#)
- [Critical Infrastructures and Services](#)
- [CSIRT Services](#)
- [CSIRTs and communities](#)
- [CSIRTs in Europe](#)
- [Cyber Crisis Management](#)
- [Cyber Exercises](#)
- [Cyber Security Education](#)
- [Data Protection](#)
- [Incident Reporting](#)
- [IoT and Smart Infrastructures](#)
- [National Cyber Security Strategies](#)
- [NIS Directive](#)
- [Standards and certification](#)
- [Threat and Risk Management](#)
- [Trainings for Cyber Security Specialists](#)
- [Trust Services](#)

## Latest news [All news](#)



### Forest for the trees: an IoT security standards gap analysis

Published on January 17, 2019. [Read more](#)

### Forest for the trees: an IoT security standards gap analysis

Published on January 17, 2019

### Acceptance of eIDAS audits: Global or local?

Published on January 15, 2019

### Supporting the Fight Against Cybercrime: ENISA report on CSIRTs and Law Enforcement Cooperation

Published on January 09, 2019

### EU improves its capacity to tackle cyber crises: Cyber Europe 2018 after-action report

Published on December 20, 2018

### European research and development priorities in cybersecurity

Published on December 19, 2018

## Trainings for Cyber Security Specialists

- ^ Online training material
- > Legal & Cooperation
- > Setting up a CSIRT
- > Operational
- > Technical
- > Training Courses
- > Train the trainer programme
- > How to get a training

## Training Resources

Published under Online training material

Tagged with Training

## Training Resources

ENISA CSIRT training material was introduced in 2008. In 2012, 2013 and 2014 it was complemented with new exercise scenarios containing essential material for success in the CSIRT community and in the field of information security. In these pages you will find the ENISA CSIRT training material, containing Handbooks for teachers, Toolsets for students and Virtual Images to support hands on training sessions.

In order to deliver trainings more efficiently with better and longer lasting results, the following resources can be used.

- Good practice guide on training methodologies
- Roadmap to provide more proactive and efficient CSIRT training

The ENISA CSIRT training material covers four main areas:

	Topics
Technical	<ul style="list-style-type: none"><li>• Building artefact handling and analysis environment</li><li>• Processing and storing artifacts</li><li>• Artefact analysis fundamentals</li><li>• Advanced artefact handling</li><li>• Introduction to advanced artefact analysis</li><li>• Dynamic analysis of artefacts</li><li>• Static analysis of artefacts</li><li>• Forensic analysis: Local Incident Response <a href="#">New</a></li><li>• Forensic analysis: Network Incident Response <a href="#">New</a></li><li>• Forensic analysis: Webserver Analysis <a href="#">New</a></li><li>• Developing Countermeasures</li><li>• Common framework for artefact analysis activities</li><li>• Using indicators to enhance defence capabilities</li><li>• Identification and handling of electronic evidence</li><li>• Digital forensics</li><li>• Mobile threats incident handling</li><li>• Mobile threats incident handling (Part II)</li><li>• Proactive incident detection</li><li>• Automation in incident handling</li><li>• Network forensics</li><li>• Honeypots</li><li>• Vulnerability handling</li><li>• Presenting, correlating and filtering various feeds</li></ul>

## References

- Good practice guide on training methodologies
- Roadmap to provide more proactive and efficient CSIRT training
- Technical
- Building artefact handling and analysis environment
- Processing and storing artifacts
- Artefact analysis fundamentals
- Advanced artefact handling
- Introduction to advanced artefact analysis
- Dynamic analysis of artefacts
- Static analysis of artefacts

Show 38 more

# Cyber-Sec... Objetivos:

Protección de los sistemas de información a través de **medidas técnicas y organizativas**.

Las medidas a implantar abarcan, tanto medidas de **seguridad física** (edificio, personal de seguridad, sistemas de control de acceso físico, etc.) como de **seguridad lógica** (generación de logs, control de acceso lógico de aplicaciones, realización periódica de hacking ético, etc.).

Los principales objetivos que se cubren, según CCN-STIC-400:

- Confidencialidad
- Integridad
- Disponibilidad.

# Cyber-Sec... Objetivos:

- **Confidencialidad:**
  - Evitar el acceso de usuarios no autorizados a sistemas lógicos y físicos.
- **Integridad:**
  - Capacidad que garantiza que los sistemas van a preservar cualquier modificación de los datos almacenados en los sistemas.
- **Disponibilidad:**
  - Capacidad que garantiza el funcionamiento de los sistemas, existiendo procedimientos para recuperar la operativa en caso de contingencia.



ILUSTRACIÓN 2 - Seguridad de la Información según la Norma ISO/IEC 17799

Fuente: <http://www.itsteziutlan.edu.mx>

# Cyber-Sec... Objetivos:

## Dimensiones adicionales:

- Trazabilidad.
- No repudio.
- Autenticidad.

## Factores (internos y externos):

- Planes de negocio y el entorno empresarial.
  - Naturaleza del negocio, perfil de seguridad, tolerancia al riesgo, tendencias de la industria, fusiones, adquisiciones y partnerships, outsourcing y proveedores.
- La tecnología de la información disponible en la entidad (herramientas, conexión, etc.)
  - Particularidades del proceso o sistema: herramientas, conexiones, complejidad de la estructura IT, soporte operacional para seguridad, usuarios y sus capacidades y herramientas de seguridad.

## Cyber-Sec... Objetivos:

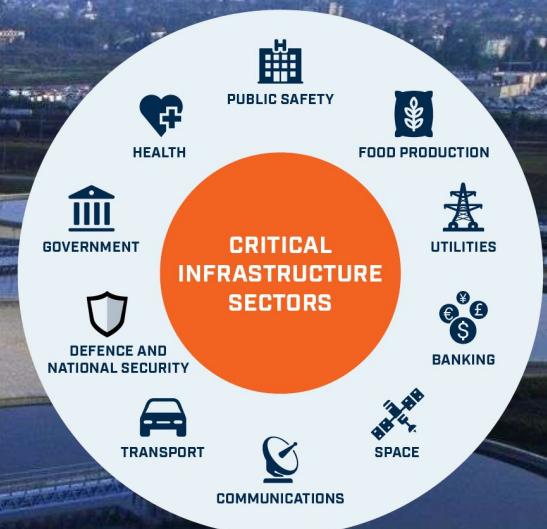
- Proteger el principal activo de cualquier organización.

A scene from the movie Indiana Jones and the Last Crusade. Indiana Jones, played by Harrison Ford, is wearing his signature fedora and leather jacket. He is crouching in a dark, rocky environment, looking intensely at a large, glowing golden Ark of the Covenant. The Ark is rectangular with vertical stripes and a prominent gold plate on top. A thick, dark smoke or mist surrounds the Ark and Jones, creating a mysterious atmosphere.

La información



# El proceso productivo



# Infraestructuras críticas





# EL ARTE DE LA GUERRA

---

# SUN TZU

LAS VICTORIAS DE LOS BUENOS  
GUERREROS NO SE DEBEN A LA SUERTE,  
SINO A HABERSE SITUADO PREVIAMENTE  
EN POSICIÓN DE GANAR CON SEGURIDAD,  
IMPONIÉNDOSE SOBRE LOS QUE  
YA HAN PERDIDO DE ANTEMANO.

## Cyber-Sec... Antecedentes:

Estados y empresas logran ventajas sobre sus competidores, obteniendo información privilegiada o perjudicando a sus rivales, ocasionando pérdidas económicas o de imagen, tras atacar su infraestructura o conseguir el robo y la exfiltración de información confidencial.

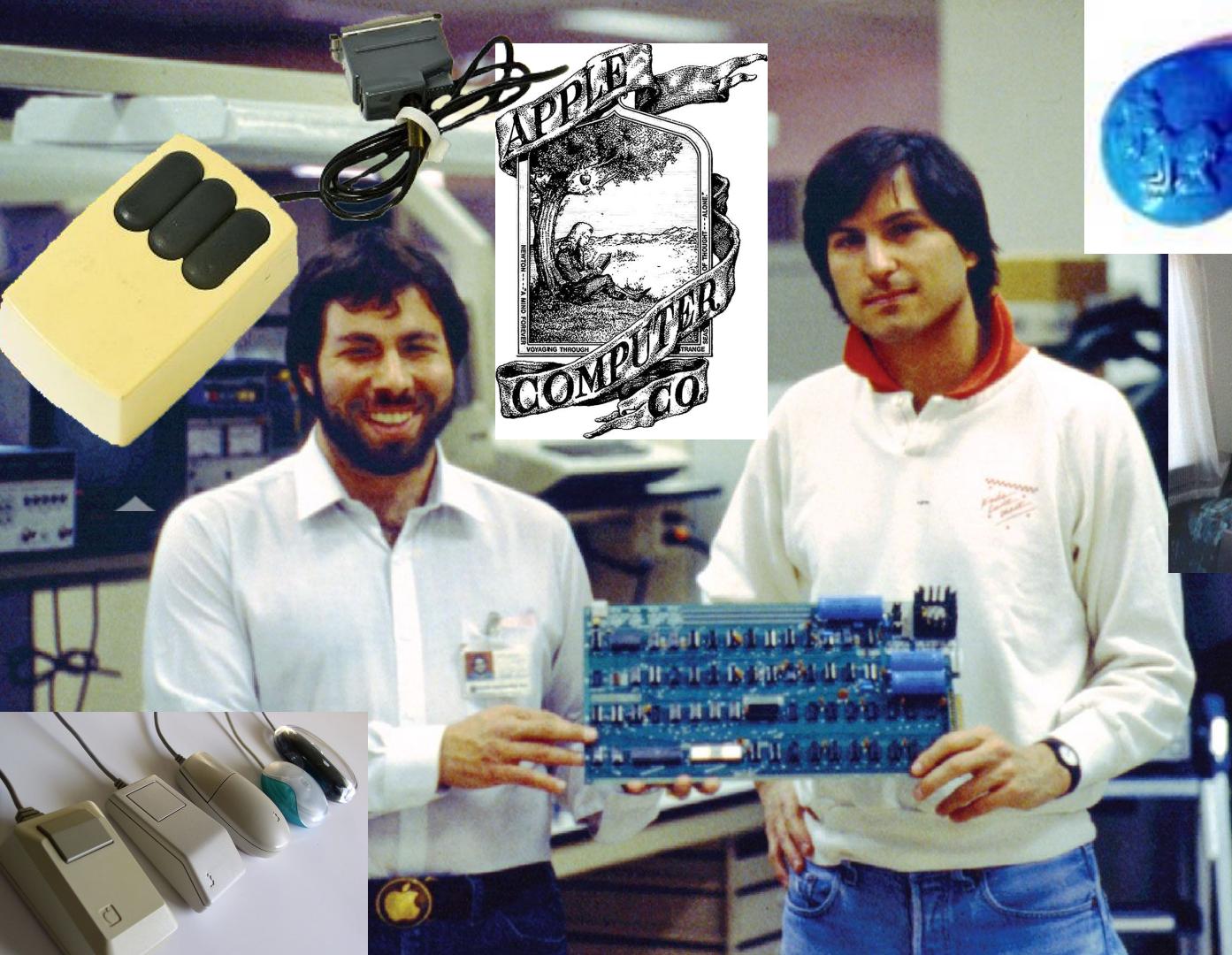
# **PIRATES of SILICON VALLEY**

[PLAY MOVIE](#)

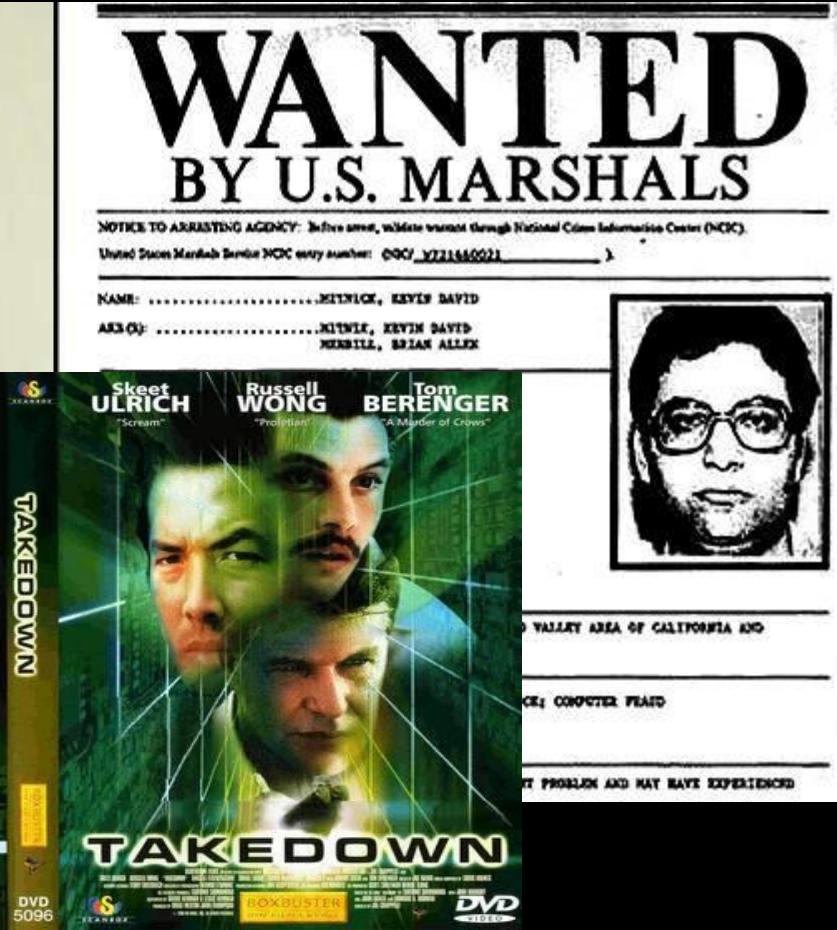
[SCENES](#)

[FEATURES](#)

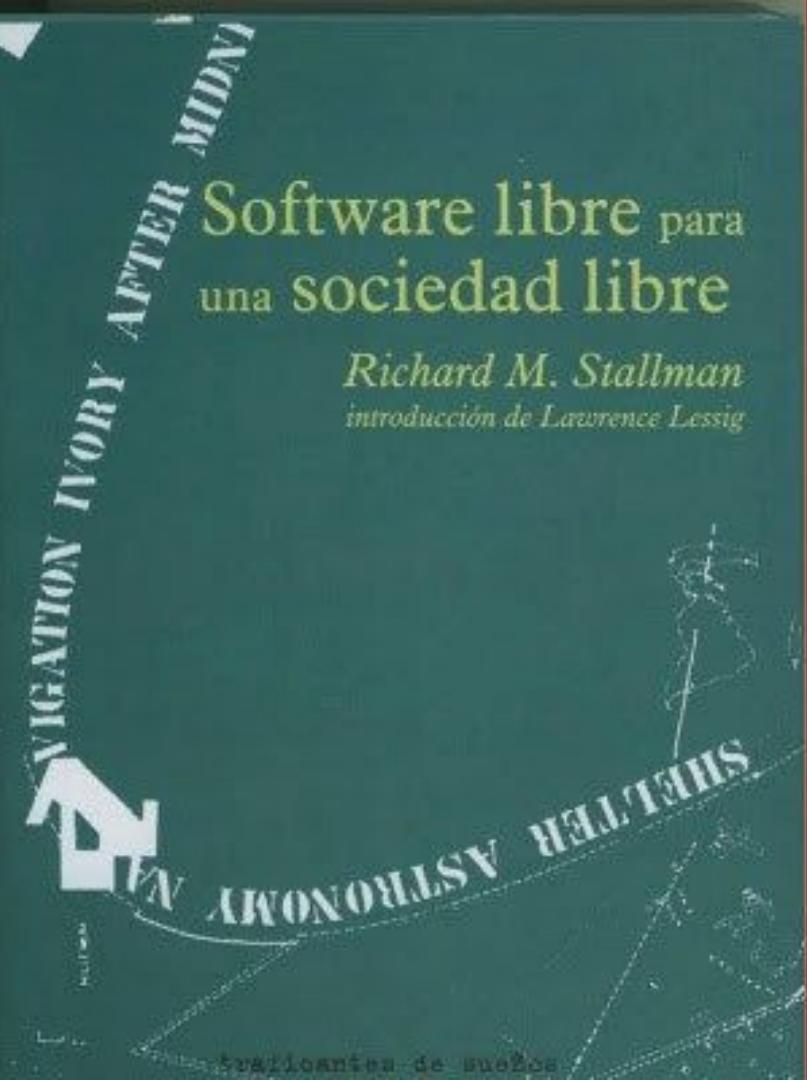
[LANGUAGES](#)







FREE KEVIN

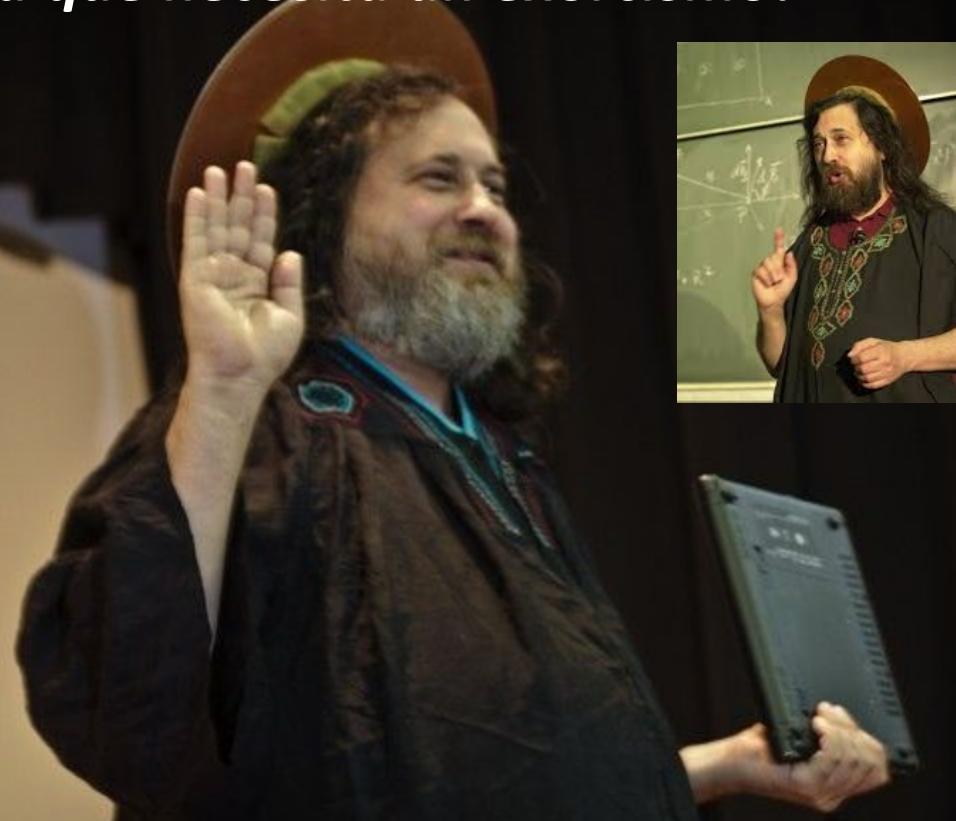


# Free Software, Free Society

Selected Essays of Richard M. Stallman  
Second Edition



*- Soy San iGNUcius, de la iglesia de Emacs.  
Bendigo tu computadora, hijo mío. ¡Veo una  
computadora que necesita un exorcismo!*



## Invasiones en ordenadores de América y Asia

El pasado 2 de marzo, 14 de los 25 centros informáticos de la NASA, incluyendo la central de Washington, sufrieron ataques de hackers. En aquella ocasión se produjeron pérdidas. Los sistemas afectados fueron: Unix, Macintosh, Amiga NT y Windows 95.

Para realizar el ataque según las fuentes consultadas, los hackers utilizaron los técnicos conocidos como invasores, zonas y puertos. Algunos de ellos se comunicaron mediante correo electrónico. Al parecer, este ataque fue una respuesta por la detención de dos jóvenes piratas que obtuvieron acceso a varias máquinas del Gobierno de EE.UU. que contenían información confidencial.

En el caso de la Escuela Politécnica de la Universidad Nacional EZLN, protagonista en febrero la página del Maestro de Hacienda de México. Hacían ciberataques repletos de errores en la web de la Secretaría de Hacienda y Crédito Público. El ataque fue llevado a cabo por un grupo de piratas informáticos llamados "X-Pat".

Quien atendió no pertenece al EZLN, aunque otras fuentes señalan su vinculación con el movimiento zapista. El grupo renombró la página con imágenes de la revolución mexicana de 1910. Timoño Zapata y mensajería del subcomandante Marcos. La mayoría se protegió durante toda la noche del 2 de abril.

En julio, un grupo de piratas accedió sin internet a los datos de 100 mil de un banco y se llevó 100 mil a cuenta. Los ciberautomáticos se robaron con impunidad durante una semana y los dependientes vivieron de la entrada.



Maki (izquierda) y Angelico continúan con su página presente en Internet.

## Jamón, vino y Timofónica

'Webs' de protesta contra Telefónica llevan al juzgado a varios internautas

### E.S.A. Barcelona

**A**ngel Badía, Angelico y Francisco Salazar celebran el primer aniversario de su grupo de hackers, los lejos de la informática y de Internet. Su sitio y todos los que han causado problemas con la policía. Su página Web <http://www.islatortuga.com> es una de las más visitadas. A través de su servidor distribuyen una página para denunciar a Telefónica Viva el jamón y el vino. "Es una persecución. Somos inocentes", aseguran. Los tres internautas se consideran los padres de la página que ha resuelto los problemas de la empresa. Lo que hacen es legal, venen los diarios, algo que ya se acuerda. El periodista Mariano Álvarez, director de la revista de la información, ha comentado que la empresa ha presentado una denuncia por uso de su logotipo en páginas de Internet.

un lugar de la red y la pongo aquí. Así os ahorraré las horas de 'yo he gastado en bocadillo buenisimo'".

Angelico y Maki celebraron el primer aniversario de su grupo el 27 de marzo, "nos incudieron ordenadores y nos dejaron en la miseria", proceden en sus actuales páginas locos seguros. "Nosotros no construimos la página, sino que fue otra persona que sólo declaró ante el juez. Lo que hacemos es legal", venen los diarios, algo que ya se acuerda.

La policía, incluso al 4 de mayo en Ilamenes Gómez y en Legazpi, Madrid y a Juan Antonio M. K., a quien ya se acuerda, y Alberto R. R. el 27, se acuerda con este ataque. En una nota oficial, la policía dice que ha presentado una denuncia a Francisco Salazar Martínez, aunque señala que "era ajeno a los nuevos hechos detectados".

A pesar de todo, Angelico y Maki están

### LA TERMINOLOGÍA

Una jerga para la comunicación entre iniciados

Los hackers tienen una serie de códigos para comunicarse entre sí. Es como un diccionario, con conceptos como estos:

► BUG. Defecto de sistema. Un bug es un fallo del software que hace que los creadores no lo hayan detectado. Puede producirse por un error en una fórmula matemática o por un defecto en la forma de leer y tratar la información que se recibe. Consecuencias: errores de contabilidad y acceso a información restringida.

► XPLOIT. Programa que utiliza un bug para provocar determinados efectos, como conseguir información privada mediante un servidor de correo electrónico.

► WAREZ. Término que define la recopilación de intercambio de software comercial sin compartir y sin pagar derechos de autor.

► GAMEZ. Warez de videojuegos.

► HACKER. Tradicionalmente se considera hacker al aficionado a la informática cuya afición es buscar defectos y posibles trastornos para entrar en los sistemas. Para los especialistas, la definición correcta sería: experto que puede conseguir de un sistema informático cosas que sus creadores no imaginaron.

► CRACKER. Hacker cuya ocupación es buscar la forma de entrar en sistemas y los fallos de seguridad de programas.

► PHREAKER. Hacker especializado en teléfono. Su propósito es robar la tarifa de teléfono por el procedimiento de descubrir y utilizar cualquier truco que le permita rea-

### 2 TEMA DEL DÍA



Lunes, 1 de junio de 1998  
Intrusos en la red  
Tema del día



Vacio legal  
Abogados y jueces consideran que todavía existe un vacío legal en España para perseguir algunos delitos específicos que pueden cometerse a través de Internet

Lunes, 1 de junio de 1998 d Periódico

# Los 'ciberpiratas' españoles se cuelan en la NASA y el Pentágono

Un estudiante de la Politécnica entró en un satélite y movió sus placas solares

Otro 'hacker' manipuló el simulador de guerra atómica de Estados Unidos

Los saboteadores han espiado a importantes proveedores de Internet

### E.I. ALBALAT

**L**os ciberpiratas informáticos que han dejado huellas en ordenadores de la NASA, del Pentágono, del Comité Olímpico y de varios universidades y los más importantes gobiernos nacionales y de otros países, están siendo juzgados legalmente en Estados Unidos. Hoy se ha iniciado el juicio contra el cibercriminal de guerra nuclear de Estados Unidos. En la sala de los juzgados de Boston se ha iniciado la primera fase del juicio, que durará hasta el viernes. De acuerdo con las acusaciones, el hacker estadounidense que tiene como nombre de usuario Maxi ha accedido hoy a través de la red Internet a la base de datos de la Agencia Espacial Europea (esa) y ha manipulado la información que se almacenaba en los ordenadores de esa agencia. Los miembros de esa institución en los momentos en que se realizó el ataque, venían de rendir honor a los cibercriminales que han atacado sus sistemas. La Guardia Civil y la policía de Madrid ya tienen su nombre: La coppia de Maxipat, por nombre. todavía no ha sido de su autor, aunque se piensa que es el cibercriminal más conocido de Europa.

**NOTICIAS DE HACKERS**

**IHSIPAHACK**  
Los padres del computador underground en Castellano

**BLOQUEAR & CRACKER & FORENSE & ANALIZAR**

**NOTICIAS DE INTERNET**

**CODIGO EN CRIPTOGRAFIA**

**DILIGENCIA DE INFORME**

—En Barcelona, siendo las 16:30 horas del 25 de Marzo de 1998, el Instructor de las presentes hace constar el siguiente informe a SS:

—Con fecha de 2 de noviembre de 1997 se recibió en la sede de este grupo de delincuentes informáticos en Madrid un mensaje de correo electrónico a través de Internet, en el cual se adjuntaba la dirección de Internet donde podían verse diversas fotografías de los miembros de un grupo de "hackers" o intrusos informáticos que se autodenominan HISPAHACK, los cuales al parecer habían accedido de forma ilegal al ordenador del Congreso de los Diputados en Madrid.

—Puestos en contacto con el responsable técnico de dicho ordenador, éste confirmó los hechos, manifestando que, él o los atacantes habían modificado diversa información firmando los autores del acceso no autorizado como IHSIPAHACK o IH. Dicha persona, tras ser informada de la posibilidad de denunciar los hechos, participó que estudiaría las posibles acciones legales y en caso de querer denunciar se pondría en contacto con esta Unidad, no habiéndose producido tal circunstancia hasta el día de la fecha.

Dos personas fueron apresadas en Cádiz y otra en Asturias — Los agentes afirman que de la Nasa y de la Universidad de Oxford — Uno de los detenidos asegura que

## Hispahack: tres «cerebros» en la cárcel

*La Guardia Civil detiene a tres «intrusos» informáticos españoles e impone a otros diez*

MIREIA DRAGO

MADRID — Tresen 21, 22 y 26 años. Entre el miércoles y el jueves fueron detenidos por invadir los sistemas informáticos de la Nasa, de la Universidad de Oxford y de diversos centros españoles. Forman

una manada en incursiones ilegales en sistemas informáticos y en daños a proveedores de Internet, si bien la Guardia Civil, hasta ahora, sólo admite que han resultado pruebas contra los tres detenidos.

El teniente Amador del Moral cuenta que la investigación partió de la denuncia de un proveedor de



### La «red Hispahack»

Dos expertos en informática operaban desde Gibraltar, otro desde un pueblo asturiano y otra docena de personas desde distintas localidades de Cataluña.

► **Definición de «hacker»:** Gran aficionado a la informática, que accede a sistemas de ordenadores ajenos sin ánimo de lucro.

# Cuatro piratas españoles burlan el control de la NASA y acceden a su red informática

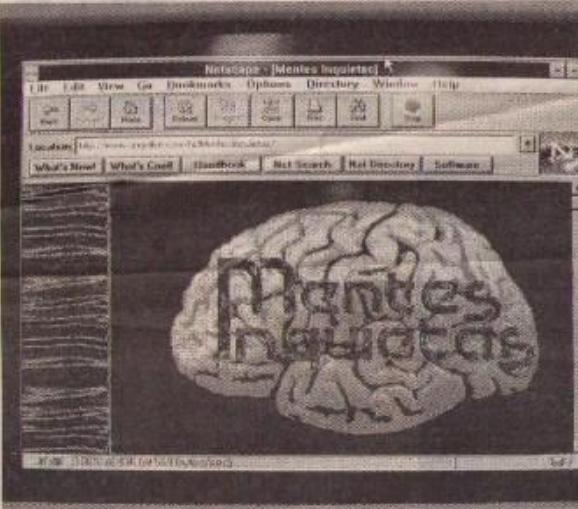
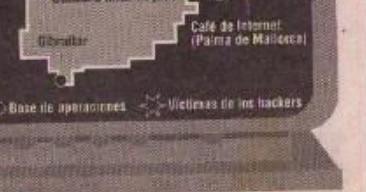
## SUCESOS

■ Tres de los detenidos son de Barcelona. El mayor no supera los 26 años. La Guardia Civil los considera unos genios

CARLOS NOVO  
DOMINGO MARCHEÑA

BARCELONA — El grupo español Os Resistentes tiene una canción titulada "Hay un hacker en la Luna". Si quieren, podrían cantar también "Hay un pirata español en la NASA". Hasta ahora, películas como "Jugos de guerra" o "La red", con genios capaces de robar los sistemas informáticos —supuestamente— más seguros del mundo, tenían protagonistas angloajunas. Dentro de poco, podrán ser latinos. El próximo viernes, va bien. La Guardia Civil ha detenido a cuatro jóvenes vascos de los ordenadores, de entre 18 y 26 años, acusados de acceder a la red informática de la agencia espacial estadounidense.

No hay constancia de que esa acción causara el más mínimo daño, pero a los acusados, que quedaron en libertad sin embargo, algunos incluso antes de declarar ante el juez, se les imputan otros delitos que sí lo hacen: 2 mil 2 plazas.



Detalle de la web que el grupo Mejores Inquietos tenía en la red

pensad en las consecuencias". Pero más adelante se dan recomendaciones en caso de ser sorprendidos por la policía: "Nunca estés de más con tu presencia. Los consejos porque aunque no nos guste, algún día los piaremos necesitar".

Las detenciones se practicaron en la localidad barcelonesa de Sant Joan Despí, donde se detuvo a un joven de 18 años, el presunto autor material de los hechos mantenidos en la UPC; en la Línea de la Concepción (Cádiz) fueron detenidos otros dos, de 21 y 22 años, ambos naturales de Mataró; también de Barcelona, y la imputación de una empresa informática de Gijón; la cuarta detención, la de un profesor de informática de 26 años, se produjo en Avilés (Asturias). Los in-

vestigadores, que han contado con ayuda de guardias civiles de las ciudades citadas, han localizado un importante número interno de la red, gracias a la Guardia Civil, ya que se trataba de un codiciloso frío en el que residía en Lyon. Otras policías, como New Scotland Yard o el FBI, han participado en las pesquisas.

Según la Guardia Civil, "algunos de los ataques realizados a sistemas informáticos utilizados en España fueron realizados desde aquí, poniendo la ayuda de cibercabecitas conectados a Internet que estaban en Ho-

**HomePage**[Calendar](#)  
[Public Relations](#)  
[Press Releases](#)**Assistance**[Enterprise](#)  
[Service Providers](#)  
[TLD Operators](#)  
[Network Detection](#)**Information**[Introduction](#)  
[Lessons Learned](#)  
[FAQ](#)  
[Infection Distribution](#)  
[Infection Tracking](#)  
[Timeline](#)  
[Malicious Sites](#)  
[Repair Tools](#)  
2012 Conficker Domain List**Tests**[Check for Infection](#)  
(Site)  
(Site)[Testen Sie auf Conficker Infektionen](#)  
(Site)  
(Site)[Проверка наражение вирусом Conficker](#)  
(Site)  
(Site)  
[Verifica si estas infectado](#)  
ईन : విరుద్ధమైనవాడు  
[Conficker អាមេរិកា](#)  
[Vérifiez si vous êtes infectés](#)[Contact us](#)[edit Sidebar](#)

# Home Page

[« October 2015 · April 2016 »](#)**Calendar:**

- No entries for February 2016.
- No entries for January 2016.
- No entries for December 2015.

 Newest first  Oldest first

## The Conficker Working Group Lessons Learned Document

Starting in late 2008, and continuing through June of 2010, a coalition of security researchers worked to resist an Internet borne attack carried out by malicious software known as Conficker. This coalition became known as "The Conficker Working Group", and seemed to be successful in a number of ways, not the least of which was unprecedented cooperation between organizations and individuals around the world, in both the public and private sectors.

In 2009, The Department of Homeland Security funded a project to develop and produce a "[Lessons Learned](#)" document that could serve as a permanent record of the events surrounding the creation and operation of the working group so that it could be used as an exemplar upon which similar groups in the future could build. This is the document.

The Rendon Group conducted the research independently, and although a number of members of the Conficker Working Group were interviewed, and provided information to the authors, the report is the sole work product of the Rendon Group. The views and conclusions are not necessarily those of the Conficker Working Group, or any of its official or unofficial members. Nonetheless the Core Committee of the Conficker Working Group believes the report has substantial value and is pleased to provide access to the Rendon document via the Conficker Working Group Website.

An additional thank you to Rick Wesson of Support Intelligence, and David Dagon from Georgia Tech for their efforts in getting the Lessons Learned project funded.

The document can also be downloaded [here](#)

Rodney Joffe  
Chair  
Conficker Working Group

Follow up questions can be directed to the Rendon Group at the address below, as well as the following members of the Conficker Working Group Core Committee:

- The Rendon Group
- Phone: +1 202-745-4900
- trginfo@rendon.com

### Conficker Working Group Core Committee:

***The ShadowServer Foundation***

- Andre' M. DiMino
- Co-Founder and Director
- Phone: +1 914-410-6480
- Email: adimino@shadowserver.org

***Neustar, Inc***

- Rodney Joffe
- Senior Vice President
- Phone: +1 202-533-2900
- Email: rodney.joffe@neustar.biz

**On this page... (hide)**

- [The Conficker Working Group Lessons Learned Document](#)
- [Conficker Working Group Core Committee](#)
- [Check to see if you are infected](#)

**Working Group Members**

Land1  
Afriasis  
AOL  
Arbor  
Cisco  
ESI  
F-Secure  
Facebook  
Georgia Institute of Technology  
Global Domains International  
IBM-ISS  
ICANN  
Internet Storm Center  
Internet Systems Consortium  
IT-ISAC  
Juniper  
Kaspersky  
McAfee  
Microsoft  
Neustar  
NIC Chile  
OpenDNS  
SecureWorks  
Shadowserver  
Sophos  
SRI International  
Support Intelligence  
Symantec  
Team Cymru  
Trend Micro  
Version

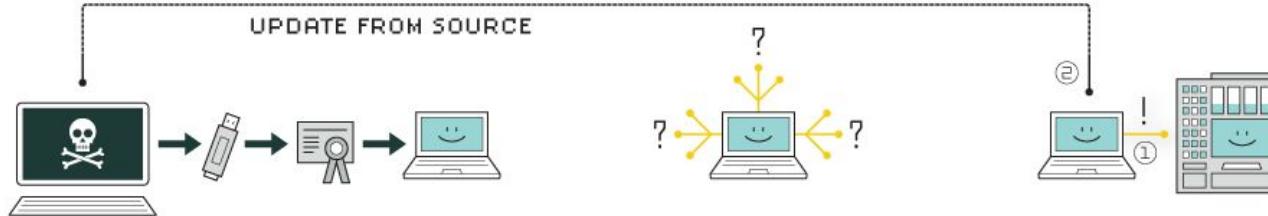
**Calendar/Blog**

November 2015  
December 2015  
January 2016  
February 2016

# Cyber-Sec... Antecedentes:

- Noviembre de 2008: Ataque del gusano **Conficker** <http://www.confickerworkinggroup.org/wiki/>.
- Junio de 2010: Ataque del gusano **Stuxnet**  
<https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet>  
<https://www.welivesecurity.com/la-es/2017/06/20/sistemas-industriales-en-la-mira/>  
<https://www.welivesecurity.com/la-es/2010/10/01/stuxnet-ataque-a-sistemas-de-control-industrial/>  
<https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra>  
<https://hipertextual.com/2010/10/stuxnet-y-el-sombrio-9-de-mayo-de-1979>  
<https://www.ecured.cu/Stuxnet>  
<https://www.symantec.com/security-center/writeup/2010-071400-3123-99>  
<https://www.ccn-cert.cni.es/ca/gestion-de-incidentes/lucia/23-noticias/1222-el-gusano-stuxnet-que-afecta-a-sistemas-scada-causa-revuelo-internacional.html>  
<https://www.elmundo.es/elmundo/2010/11/23/navegante/1290510462.html>
- Abril de 2011: **Ataque a la red PlayStation** con 23 días de caída del servicio y obtención de información personal de los usuarios de un total de 77 millones de cuentas.

# HOW STUXNET WORKED



## 1. infection

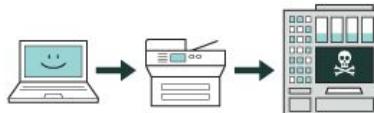
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

## 2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

## 3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



## 4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.



## 5. control

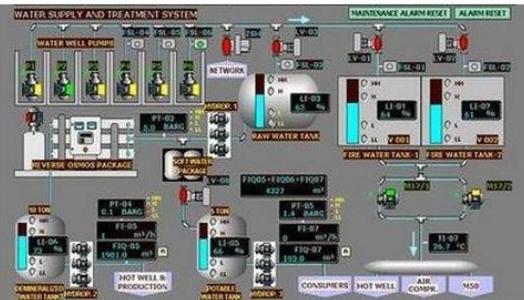
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.



## 6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

## Cyber-Sec... STUXNET:

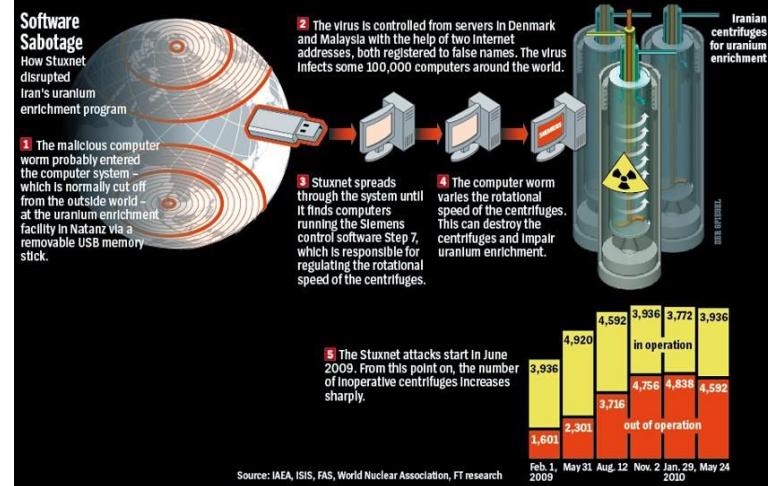


**ABC**  
El «gusano» Stuxnet ataca el sistema Scada, el software habitual en oleoductos y plantas nucleares

- Primer virus conocido que espía y reprograma sistemas industriales SCADA.
  - Objetivo PLCs de Siemens para sabotear las centrifugadoras de enriquecimiento de uranio.
  - Detectado el 17 de Junio de 2010 en la planta nuclear de Bushehr.
  - Primera infección por memoria USB y posterior propagación a través de la red.
  - Empleó un total de 4 vulnerabilidades de día cero.
  - Primer gusano en incluir un rootkit.
  - Hasta la fecha fue el malware más sofisticado del mundo.

# Cyber-Sec... STUXNET:

- Sólo funciona en dispositivos Siemens S7-300 y S7-400.
- Interviene las órdenes enviadas desde un sistema Siemens SimaticWinCC SCADA a un variador de frecuencia, y las modifica para alterar las velocidades del motor para que varíe de forma descontrolada en diferentes momentos.
- Sólo ataca a las centrifugadoras si funcionan entre los 870 y 1210 Hz.
- Al afectar la velocidad de los variadores de frecuencia, se sabotea el proceso de enriquecimiento dando como resultado un uranio de mala calidad.
- Unos investigadores infectaron un sistema conectado a una bomba de aire con un globo programado para funcionar por 3 segundos, pero Stuxnet lo prolongó hasta los 140 segundos.



# ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

[See Your Matches »](#)

Over **38,855,000** anonymous members!

# BE CAREFUL THINK BEFORE YOU ACT



As seen on: BBC News,  
Reuters, The Sun, The  
Telegraph, The Times

Ashley Madison is the  
world's leading married  
dating service for  
*discreet* encounters



Trusted  
Security  
Award



SSL  
Secure  
Site

# Cyber-Sec... Ashley Madison:

Al atacar una web se comprometen:

- Datos personales
- Pérdida de confianza de los usuarios
- Reputación
- El producto en sí mismo



En julio de 2015, un equipo de hackers denominado *Impact Team* robó datos de más de 37 millones de usuarios a la compañía amenazando hacerlos públicos si esta no cerraba inmediatamente su web.

En agosto de 2015 estos 25 Gb de datos fueron publicados en BitTorrent conteniendo datos como nombre, apellidos, teléfono, correo electrónico y transacciones financieras realizadas por los usuarios.

Como consecuencia de este escándalo, el 28 de agosto dimite Noel Biderman, su fundador.

Ready to see Hollywood's hottest A-List celebrities in all their naked and uncensored glory? Then you have come to the right place, because we publish the 100% real videos and photos the other sites don't dare show you. We keep up to date with today's hottest stars as we bring you all the naughty Tinseltown action the celebrities don't want you to see!



## DOWNLOADABLE SCANDALOUS SEX TAPES



**CLICK HERE AND GET INSTANT ACCESS!**

[home](#) > [tech](#)**Tinder**

## I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets

The dating app knows me better than I do, but these reams of intimate information are just the tip of the iceberg. What if my data is hacked - or sold?

- [Getting your data out of Tinder is really hard - but it shouldn't be](#)



35,983

**Judith Duportail**

@judithduportail

Tuesday 26 September 2017 07.10 BST



● A July 2017 study revealed that Tinder users are excessively willing to disclose information without realising it.  
Photograph: Alamy

### Most popular



Malta car bomb kills Panama Papers journalist



Men, you want to treat women better? Here's a list to start with



The Secret Actress: in Hollywood, Harvey Weinstein is not an anomaly



North Korean UN envoy says 'nuclear war may break out at any

# VICTIMA DE SEXTORSIÓN FACEBOOK?



T. +34 695 220 012 | brunoperez@evidenciesdigitals.cat  
Facebook /EvidenciesDigitals | Twitter @EvidenciesDigit  
www.evidenciesdigitals.cat



Asociación  
Stop! Violencia de  
Género Digital



## Solicita un Perito Informático

91 462 48 20  
659 082 631

INICIO LA ASOCIACIÓN ▾ HAZTE SOCIO SOLICITA UN PERITO FORMACIÓN ▾ ¿SUFRES ALGÚN TIPO DE VIOLENCIA? CONTACTO WEBINARS



Encarni Iglesias, presidenta de Stop Violencia de Género Digital: «Las chicas controlan más a su pareja»

16 diciembre, 2018



Detenido un menor por publicar en Whatsapp fotos eróticas de una niña

26 noviembre, 2018



«Sextorsión» en Galicia: «Vamos a empapelar Lugo con tus fotos»

13 noviembre, 2018



«Sextorsión» ¿Qué es y cómo evitar ser víctima de este tipo de chantaje?

7 noviembre, 2018

### Opinión de los Expertos



30 de Julio: Día Internacional contra la Trata; la esclavitud del siglo XXI

30 julio, 2018

En el año 2013, la Asamblea General de las Naciones Unidas se reunió, adoptando sus...



La prostitución: esto no va de sexo

1 febrero, 2018

Os invitamos a leer el artículo publicado en El País.com de nuestra compañera y amiga...



Opinión – Violencia de Género en los medios: de la información a la formación

7 agosto, 2017

Partimos de la base de que los medios de comunicación tienen como objetivo informar, formar...

### Síguenos Por las Redes Sociales



### Guías y Consejos contra la Violencia de Género Digital



CONSEJOS PARA PREVENIR UNA SEXTORSIÓN  
www.stopviolenciadegenerodigital.com



CONSEJOS PARA INTERVENIR EN UN CASO DE CIBERBULLYING  
www.stopviolenciadegenerodigital.com



CONSEJOS PARA EVITAR UNA SUPLANTACIÓN DE IDENTIDAD  
www.stopviolenciadegenerodigital.com



016



# Cyber-Sec... Antecedentes:

- Julio de 2015: Ataque contra la empresa **Hacking Team**. Más de 400 Gb de información de la empresa fueron comprometidos afectando a distintos clientes y gobiernos para los que la empresa ofrecía servicios de seguridad.
- Octubre de 2016: Ataque de Denegación de Servicio (DDoS) a la empresa Dyn, encargada de la infraestructura de nombres de dominio o DNS. Todas las empresas a las que Dyn daba servicio, se vieron afectadas incluyendo a organizaciones tan relevantes como Spotify o Twitter.



# GreyEnergy: uno de los actores maliciosos más peligrosos cuenta con un arsenal actualizado

Una investigación de ESET revela la presencia del sucesor del grupo de APT de BlackEnergy apuntando a infraestructuras críticas; muy probablemente en la etapa previa a la realización de un ataque.



Anton Cherepanov and Robert Lipovsky 17 Oct 2018 - 11:55AM

Compartir



Una reciente investigación de ESET reveló nuevos detalles del sucesor del grupo de APT de BlackEnergy, cuya principal herramienta fue vista por última vez en diciembre de 2015 cuando por primera vez en la historia un ciberataque fue el responsable de provocar un apagón. Cerca de las fecha del incidente, cuando cerca de 230.000 personas quedaron sin electricidad, comenzamos a detectar otra infraestructura de malware que llamamos GreyEnergy. Desde ese entonces ha sido utilizada para atacar compañías de energía, así como también otros blancos de ataque de gran valor en países como Ucrania y Polonia a lo largo de los últimos tres años.

Es importante aclarar que cuando nos referimos a "grupos de APT" establecemos conexiones sobre la base de indicadores técnicos, como pueden ser similitudes de código, infraestructura C&C compartida, cadenas de ejecución de malware, entre otras características. Por lo general, no nos involucramos directamente en la investigación y la identificación de quienes desarrollan el malware y/o que luego lo implementan o interactúan con ellos. Dado que el término "grupo de APT" suele estar más asociado con los indicadores de malware anteriormente mencionados y frecuentemente se utiliza simplemente para categorizar, nos mantenemos al margen de la especulación con respecto a la atribución de ataques a países o gobiernos.

# New Shamoon V3 Malware Targets Oil and Gas Sector in the Middle East and Europe

December 13, 2018 | Anomali Labs



A new version of destructive wiper malware Shamoon was first identified by security researchers on December 5, 2018. This malware, dubbed Shamoon V3, appears to be a new version of the destructive malware, which has historically been associated with advanced persistent threat actors aligned with the interests of the Iranian state. It has targeted at least one European oil and gas company with operations in the Middle East and Asia. Unconfirmed reports also indicate possible entities in the UAE oil and gas industry are affected as well. A defining characteristic of this new Shamoon version is that it shares nearly 80 percent similarity with earlier versions of Shamoon and may use a historic trigger date, so that it can immediately perform destructive actions once infecting a user's machine. Although not confirmed to be the work of Iranian APT groups, the malware's codebase, targeted sector, and targeted geography have all been observed in historic attacks which were later attributed to adversaries from the region.

# Cyber-Sec... Roles y responsables:



- Junta directiva (Board of directors).
  - Análisis de impacto de negocio (BIA).
- Equipo de dirección (Executive committee).
  - Director Ejecutivo (**CEO**, Chief Executive Officer).
  - Responsable de seguridad de la información (**CISO**, Chief Information Security Officer).
- Gestión de seguridad (Security Management).
  - Director de Seguridad (**CSO**, Chief Security Officer).
    - plan de continuidad del negocio (BCP, Business Continuity Plan).
    - plan de recuperación de desastres (DRP, Disaster Recovery Plan).
- Especialistas de seguridad (Cyber security practitioners).

MUNDO  
MÁS TÉCNICO

MUNDO  
MENOS TÉCNICO



ILUSTRACIÓN 2 - Evolución entre los perfiles técnicos

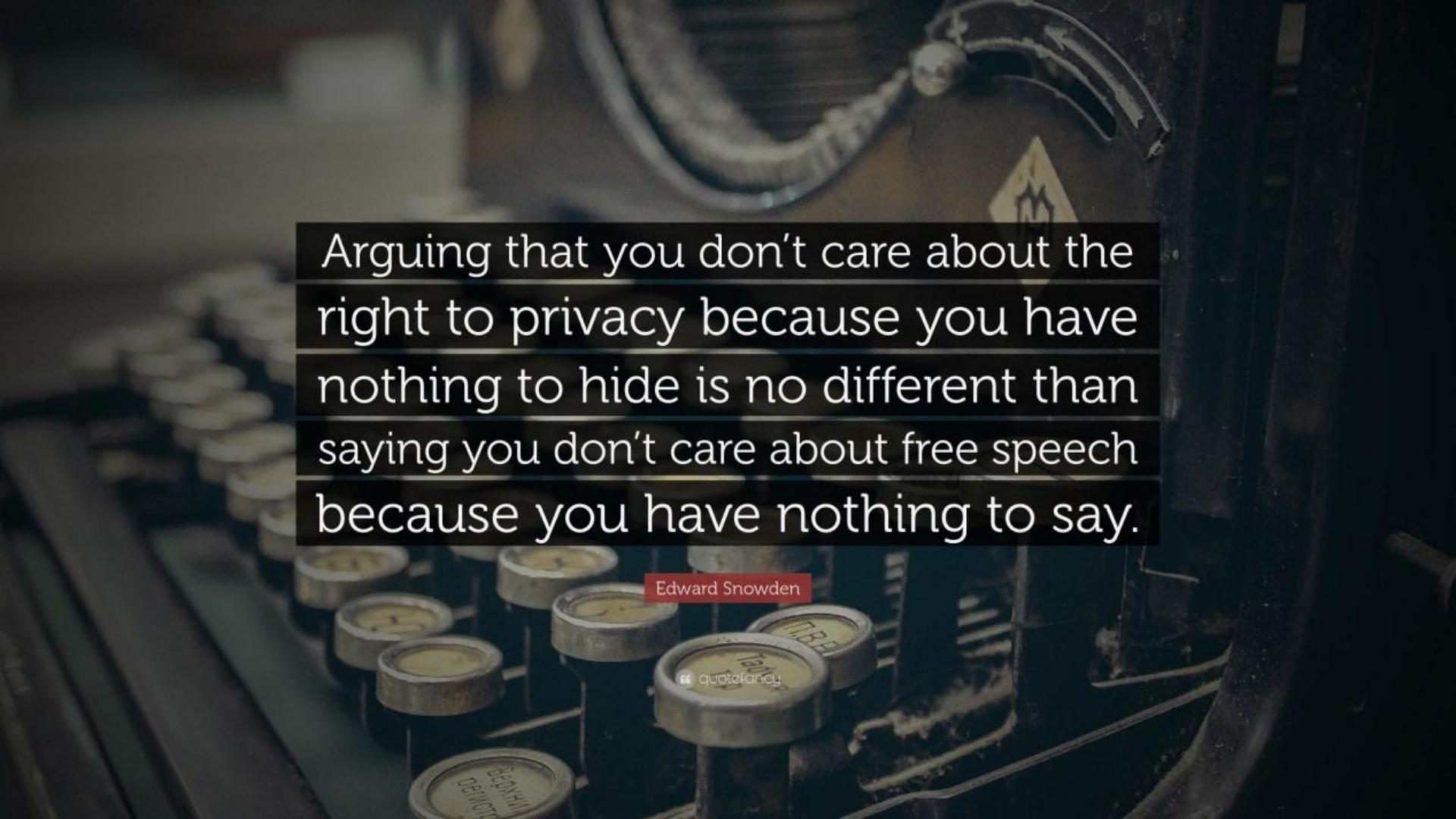
# Cyber-Sec... Perfiles técnicos:

- Analista forense, perito, etc.
- Pentester (test de intrusión).
- Arquitecto de seguridad.
- SecAdmin (Respuesta a incidentes).
- Cumplimiento normativo:
  - Administración del riesgo.
  - Administración Cumplimiento.
  - Protección de datos.
  - Continuidad de negocio.









Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.

Edward Snowden

quotefancy



ILUSTRACIÓN 5 - Plan de Respuesta a Incidentes  
Fuente: NIST

# RESPUESTA A CIBERATAQUES

## Saguaro

Actor mexicano enfocado en el robo de credenciales. Más de 60.000 IPs diferentes afectadas y más de 36 países afectados.

## STRUTS

Vulnerabilidad que afectó a millones de servidores web conectados a Internet. En España, 75 organismos afectados, seis de ellos con impacto crítico.

## NotPetya

Ataque a la cadena de suministros en Ucrania con robo de credenciales. Empleo del exploit Eternalblue para su propagación.

Enero 2017

Febrero 2017

Marzo 2017

Mayo 2017

Junio 2017

Octubre 2017

## Owncloud

Suite que permitía tener un servidor en una nube privada. Explotación de varias vulnerabilidades, acceso a archivos y ejecución de código. Diez entidades afectadas. Algunas de ellas siguen siendo vulnerables.

## Wannacry

El CCN desarrolló la vacuna NoMoreCryv0.1. y además publicó un informe de código dañino, Ransom. WannaCry. A día de hoy, se sigue actualizando la herramienta.

## #OpCatalunya

Campaña de cuatro fases contra AAPP y empresas. Ataques de DDoS a más de 70 páginas. Además, se emplearon las redes sociales para aumentar la visibilidad y coordinación.



Payment will be raised on

5/15/2017 16:32:52

Time Left

02:23:58:49

### What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

### Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

Your files will be lost on

5/19/2017 16:32:52

Time Left

06:23:58:49

### How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)



Send \$300 worth of bitcoin to this address:

12H9YD9gmcwZ9t4yMgvw41Sp7AABmugfS3Mw...

Copy

[Check Payment](#)

[Decrypt](#)

# Cyber-Sec... WannaCry: Vulnerabilidad del protocolo SMB de Microsoft CVE-2017-0144

 Go to tool  
CVE Search  
Advanced Search

[Home](#) > [CVE](#) > [CVE-2017-0144](#)

[Search CVE List](#) [Download CVE](#) [Data Feeds](#) [Request CVE IDs](#) [Update a CVE Entry](#)  
**TOTAL CVE Entries: 111064**

[Printer-Friendly View](#)

**CVE-ID**  
**CVE-2017-0144** [Learn more at National Vulnerability Database \(NVD\)](#) • [CVSS Severity Rating](#) • [Fix Information](#) • [Vulnerable Software Versions](#) • [SCAP Mappings](#) • [CPE Information](#)

**Description**  
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

**References**  
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.  

- EXPLOIT-DB-42030
- URL:https://www.exploit-db.com/exploits/42030/
- EXPLOIT-DB-42031
- URL:https://www.exploit-db.com/exploits/42031/
- EXPLOIT-DB-41891
- URL:https://www.exploit-db.com/exploits/41891/
- EXPLOIT-DB-41987
- URL:https://www.exploit-db.com/exploits/41987/
- MISIC:https://ics-cert.us-cert.gov/advisories/ICSMIA-18-058-02
- CONFIRM:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa\_701903.pdf
- CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa\_966341.pdf

**BID**  
• BID-704

**URL**  
• URL:https://www.securityfocus.com/bid/95704

**SECTRACK**  
• SECTRACK-1037991

**SEARCH CVE USING KEYWORD:**    
You can also search by reference using the [CVE Reference Maps](#).

**Comments (Legacy)**

**Proposed (Legacy)**  
N/A

This is an entry on the [CVE List](#), which provides common identifiers for publicly known cybersecurity vulnerabilities.

**SEARCH CVE USING KEYWORD:**    
You can also search by reference using the [CVE Reference Maps](#).

**For More Information:** [cve@mitre.org](mailto:cve@mitre.org)

[BACK TO TOP](#)

# Cyber-Sec... WannaCry:

## Vulnerabilidad del protocolo SMB de Microsoft CVE-2017-0144



# NSA's Target List Leaked!

- Actualización de seguridad publicada el 14 de marzo de 2017.
  - Empleo del exploit *EternalBlue*, supuestamente desarrollado por la NSA.
  - Filtrado el 14 de abril de 2017 por el grupo de hackers *Shadow Brokers*.
  - Ataque a escala mundial el 12 de mayo de 2017.
  - Ha recaudado 116555 €.

**actual ransom** (@actual\_ransom)

This bot is watching the bitcoin wallets tied to the #WannaCry ransomware attack. USD amounts as of time of tweet. By @collinskeith. More: [qz.com/862993](http://qz.com/862993)

Inside a raspberry pi

**Status of WannaCry**  
51.98076422 BTC (\$  
337 payments, 0 with  
Last payment:  
2017-06-28 at 05:50

Traducir del inglés

5:07 - 30 jun. 2017

# Cyber-Sec... WannaCry:

Atribución:

- Código compartido con Lazarus Group
- De todos los idiomas, el mejor escrito es el chino



<https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/>

<http://blog.elevenpaths.com/2017/06/wannacry-chronicles-messi-coreano.html>



VirusTotal es un servicio gratuito que **analiza archivos y URLs sospechosas** facilitando la rápida detección de virus, gusanos, troyanos y todo tipo de malware.

Archivo

URL

Buscar

No hay archivo seleccionado

**Seleccionar**

Tamaño máximo: 128MB

Al hacer click en 'Analizar', acepta nuestros [Términos del servicio](#) y permite que VirusTotal comparta este fichero con la comunidad de seguridad. Vea nuestra [Política de privacidad](#) para más detalles.

**Analizar**

## Época Romántica (1996-2000)

- Virus destructivos
- Carácter local, sin propagación
- Creación de Virus
- Personas solitarias, muy localizadas

**MOTIVACIONES:**  
Superación personal  
Conocimientos técnicos

**Origen:**  
Personas individuales o grupos muy pequeños

**A destacar:**  
Alta calidad técnica  
No hay programación

## Edad Media (2001-2004)

- Primeros phishing (11S)
- Gusanos
- Botnets 1.0 (IRC)

**MOTIVACIONES:**  
Dinero rápido  
Infecciones masivas

**Origen:**  
Personas individuales o grupos muy pequeños

**A destacar:**  
Baja calidad técnica  
No hay programación

## Fraude (2005-2006)

- Milicias cibernéticas
- Múltiples objetivos
- Control del 50% de los ordenadores

**MOTIVACIONES:**  
Dinero de cualquier forma  
Extorsiones

**Origen:**  
Personas individuales o grupos muy medianos

**A destacar:**  
Phishing y malware  
100% fraude bancario

## e-crime (2007-2009)

- Ataques geopolíticos
- Botnets 2.0
- ISP a prueba de balas
- Infraestructura en venta
- Iframe businesss, pay per install, clickfraud, botnets, DDoS, infection kits, C&C, cyberwarfare, espionaje industrial...

**MOTIVACIONES:**  
Controlar Internet  
Dominación total

**Origen:**  
Grupos de crimen organizado

**A destacar:**  
Target: gobiernos, empresas  
Amenazas políticas

# MALWARE...

- Definición de Malware:
  - (Programa/código) software malicioso o molesto. LLeva a cabo acciones sin conocimiento del usuario.
  - Objetivo: Obtener información sensible y ganar acceso a sistemas privados.
  - Capacidades para:
    - Alterar el contenido de sistema.
    - Capturar datos confidenciales.
    - Propagarse a otros sistemas.
- Tipología.
- Tendencias de ataque hoy día.

# MALWARE...

## Perjuicios:

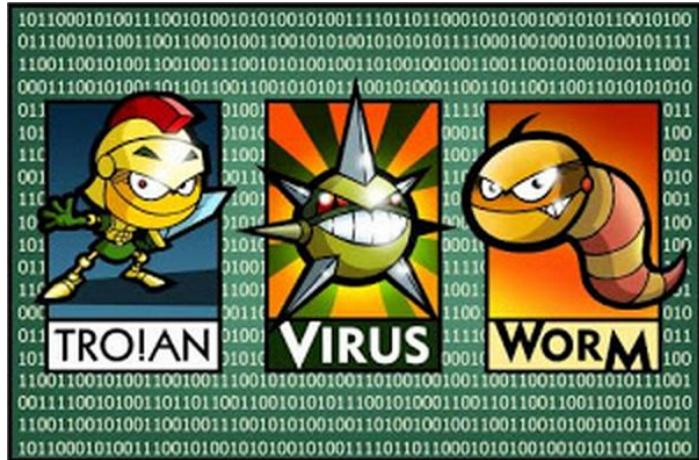
- Envío de correo a gran escala.
- Eliminación de archivos.
- Modificación de archivos.
- Degradación del rendimiento.
- Inestabilidad del sistema.
- Robo de información corporativa y confidencial.
- Modificación de la configuración de seguridad.



# MALWARE...

## Tipología:

- Virus: Se integra dentro de otro, Crea copias de sí mismo.
- Gusano: Propagación automática/autónoma. Ocultación.
- Troyano: C&C, RAT, backdoor, etc.
- Rootkit: Se oculta a sí mismo:
  - modo usuario.
  - modo Kernel.
- Botnet



- ♦ Blog
- ♦ Avisos de seguridad
- ♦ RGPD para pymes
- ♦ ¿Qué te interesa?
- ♦ Kit de concienciación
- ♦ Hackend
- ♦ Políticas de seguridad
- ♦ Juego de Rol
- ♦ ¿Conoces tus riesgos?
- ♦ Formación
- ♦ Guías
- ♦ Sellos de confianza
- ♦ Formulario de contacto

## Línea de Ayuda

¿Has tenido un incidente de ciberseguridad? Contacta: **900 116 117**

## ¿Aplicas el RGPD?

¡Las claves para cumplirlo y conseguir más confianza en tu negocio!

## ¡A la carta!

¿Sabes cómo se protegen las empresas de tu sector?

## Servicio Antibotnet

Una botnet es un conjunto de ordenadores controlados remotamente por un atacante que pueden ser utilizados en conjunto para realizar actividades maliciosas como envío de spam, ataques de DDOS, propagar virus, y cometer otros tipos de delitos y fraudes en la Red. En nuestra empresa muchas veces **conocemos esta situación cuando el ordenador funciona muy lento o algunas aplicaciones han dejado de funcionar.**

Para que puedas comprobarlo, ponemos a disposición de tu empresa un **servicio gratuito** que permite saber de manera fácil y sencilla si algún equipo de tu empresa está infectado por una botnet.

¿Cómo funciona el servicio antibotnet para empresas?

INCIBE recopila información que permite conocer la existencia de ordenadores que forman parte de una botnet.

Las empresas que dispongan de una red de ordenadores, que analizan el tráfico de red a través de un sistema de monitorización, pueden integrar el componente facilitado por INCIBE que permite mostrar una alerta de manera automática, en el caso de que alguna de las IPs de la empresa forme parte de una botnet.

De forma más gráfica, el esquema de funcionamiento del servicio antibotnet imágenes el siguiente:

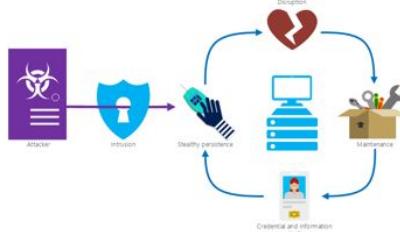
Las autoridades en colaboración con equipos de seguridad han incautado este servidor malicioso, pero es necesario que los dispositivos que controla sean desinfectados, en caso contrario los cibercriminales podrían reactivar la botnet desde otro punto. Para ello informan a las entidades competentes sobre las miles de direcciones IP públicas que se están conectando al servidor malicioso en tiempo real.



El Servicio Antibotnet chequea tu dirección IP pública contra nuestra base de datos de direcciones IP para saber si desde tu red hay alguna conexión con el servidor malicioso que controla la botnet, pero no accedemos ni podemos saber cuál de tus dispositivos es el afectado. En ningún caso monitorizamos el tráfico de tu red, ni accedemos a datos en tu ordenador.

# MALWARE... Tendencias:

Malware en memoria, sin tocar el disco



- Drive-by Download.
- Inyecciones de código (vulnerabilidades).
- Exploits kits.
- Robo de identidad / fraude: usurpación/suplantación de identidad.
- DDoS. <https://mad-rabbit.com/example-of-a-ddos-attack/>
- Phishing.
- Spam/Hoax.
- Rogueware / scareware:
- Data Breach:
- APT's.
- Watering hole.



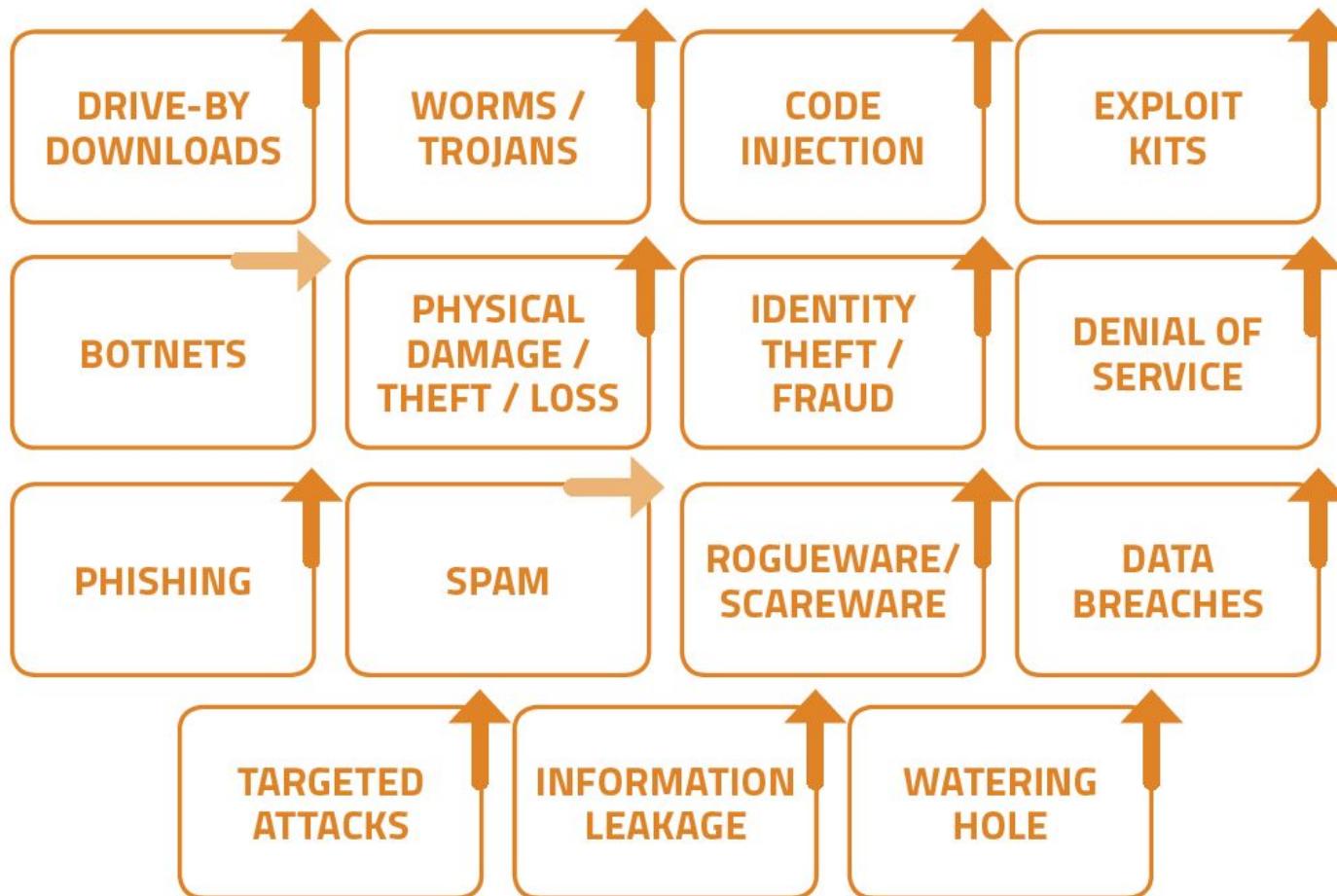


ILUSTRACIÓN 5 - Tendencias de ataques y malware

Fuente: ENISA Threat Landscape 2013



## AGENTES DE AMENAZA



## VECTORES DE ATAQUE



## DEBILIDADES DE SEGURIDAD



## IMPACTOS TÉCNICOS



## IMPACTOS AL NEGOCIO

ESPECÍFICO DE LA APLICACIÓN	EXPLOTABILIDAD FÁCIL	Prevalencia COMÚN	Detección PROMEDIO	IMPACTO SEVERO	ESPECÍFICO DE LA APLICACIÓN / NEGOCIO
Considere a cualquiera que pueda evitar información no confiable al sistema, incluyendo usuarios externos, usuarios internos y administradores.	<p>El atacante envía ataques con cadenas simples de texto, los cuales explotan la sintaxis del intérprete a vulnerar.</p> <p>Casi cualquier fuente de datos puede ser un vector de inyección, incluyendo las fuentes internas.</p> <p>Estas fallas son fáciles de descubrir al examinar el código, pero difíciles de descubrir por medio de pruebas. Los analizadores y "fuzzers" pueden ayudar a los atacantes a encontrar fallas de inyección.</p>	<p>Las fallas de inyección ocurren cuando una aplicación envía información no confiable a un intérprete.</p> <p>Estas fallas son muy comunes, particularmente en el código antiguo. Se encuentran, frecuentemente, en las consultas SQL, LDAP, Xpath o NoSQL; los comandos de SO, intérpretes de XML, encabezados de SMTP, argumentos de programas, etc.</p>		<p>Una inyección puede causar pérdida o corrupción de datos, pérdida de responsabilidad o negación de acceso.</p> <p>Algunas veces, una inyección puede llevar a el compromiso total del servidor.</p>	<p>Considere el valor de negocio de los datos afectados y la plataforma sobre la que corre el intérprete.</p> <p>Todos los datos pueden ser robados, modificados o eliminados.</p> <p>¿Podría ser dañada su reputación?</p>



# Top 10-2017 Top 10

## Translation Efforts - Otros Idiomas

[2017 Table of Contents](#)
[PDF version](#)

A1-Injection →

[← Application Security Risks](#)

## OWASP Top 10 Application Security Risks - 2017

### [A1:2017-Injection](#)

Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

### [A2:2017-Broken Authentication](#)

Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.

### [A3:2017-Sensitive Data Exposure](#)

Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.

### [A4:2017-XML External Entities \(XXE\)](#)

Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.

### [A5:2017-Broken Access Control](#)

Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.

### [A6:2017-Security Misconfiguration](#)

Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched/upgraded in a timely fashion.

### [A7:2017-Cross-Site Scripting \(XSS\)](#)

XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

### [A8:2017-Insecure Deserialization](#)

Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

### [A9:2017-Using Components with Known Vulnerabilities](#)

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

### [A10:2017-Insufficient Logging&Monitoring](#)

Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.

[2017 Table of Contents](#)
[PDF version](#)

A1-Injection →

[← Application Security Risks](#)

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	↔	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	↔	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	↔	8. Botnets	↑	↓
9. Insider threat	↔	9. Insider threat	↔	→
10. Physical manipulation/damage/theft/loss	↑	10. Physical manipulation/damage/theft/loss	↔	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

Legend: Trends: Declining, Stable, Increasing

Ranking: Going up, Same, Going down

Figure 1: Overview and comparison of the current threat landscape 2017 with the one of 2016.

# Cyber-Sec... Referencias:

OWASP



ZIBERSEGURTASUN EUSKAL ZENTROA  
CENTRO VASCO DE CIBERSEGURIDAD

- [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)
- <https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf>

<https://www.basquecybersecurity.eus/es/>

[https://www.basquecybersecurity.eus/archivos/201812/bcsc\\_libro\\_blanco\\_ciberseguridad\\_euskadi\\_es.pdf?1](https://www.basquecybersecurity.eus/archivos/201812/bcsc_libro_blanco_ciberseguridad_euskadi_es.pdf?1)

Código de Derecho de la Ciberseguridad.

[https://www.boe.es/legislacion/codigos/abrir\\_pdf.php?fich=173\\_Codigo\\_de\\_Derecho\\_de\\_la\\_Ciberseguridad.pdf](https://www.boe.es/legislacion/codigos/abrir_pdf.php?fich=173_Codigo_de_Derecho_de_la_Ciberseguridad.pdf)

▼ LIBRO BLANCO  
DE LA CIBERSEGURIDAD  
EN EUSKADI

2018




[Inicio](#) | [Avisos](#) | [Incidentes](#) | [Reportar una vulnerabilidad](#) | [Alertas](#) | [Publicaciones](#) | [Intercambio de amenazas](#) | [Otras actividades](#) | [Sobre BCSC](#)

## Ciberseguridad Industrial en Euskadi

### ACTUALIDAD BCSC



#### 102 empresas vascas reciben las primeras ayudas del Gobierno Vasco para impulsar la ciberseguridad industrial

102 empresas, 56 guipuzcoanas, 25 vizcainas y 21 alavesas, se beneficiarán este año del programa de ayudas del Gobierno Vasco para impulsar la ciberseguridad industrial pionero en nuestro entorno y que, impulsadas por el Grupo SPII, tenía una partida inicial de 600.000 euros y se ha ampliado hasta el millón de euros ante la fuerte demanda por parte de las empresas. Esta inversión pública va a servir para promover una inversión privada en ciberseguridad que alcanza los 2,34 millones euros.



#### Libro blanco de la ciberseguridad en Euskadi

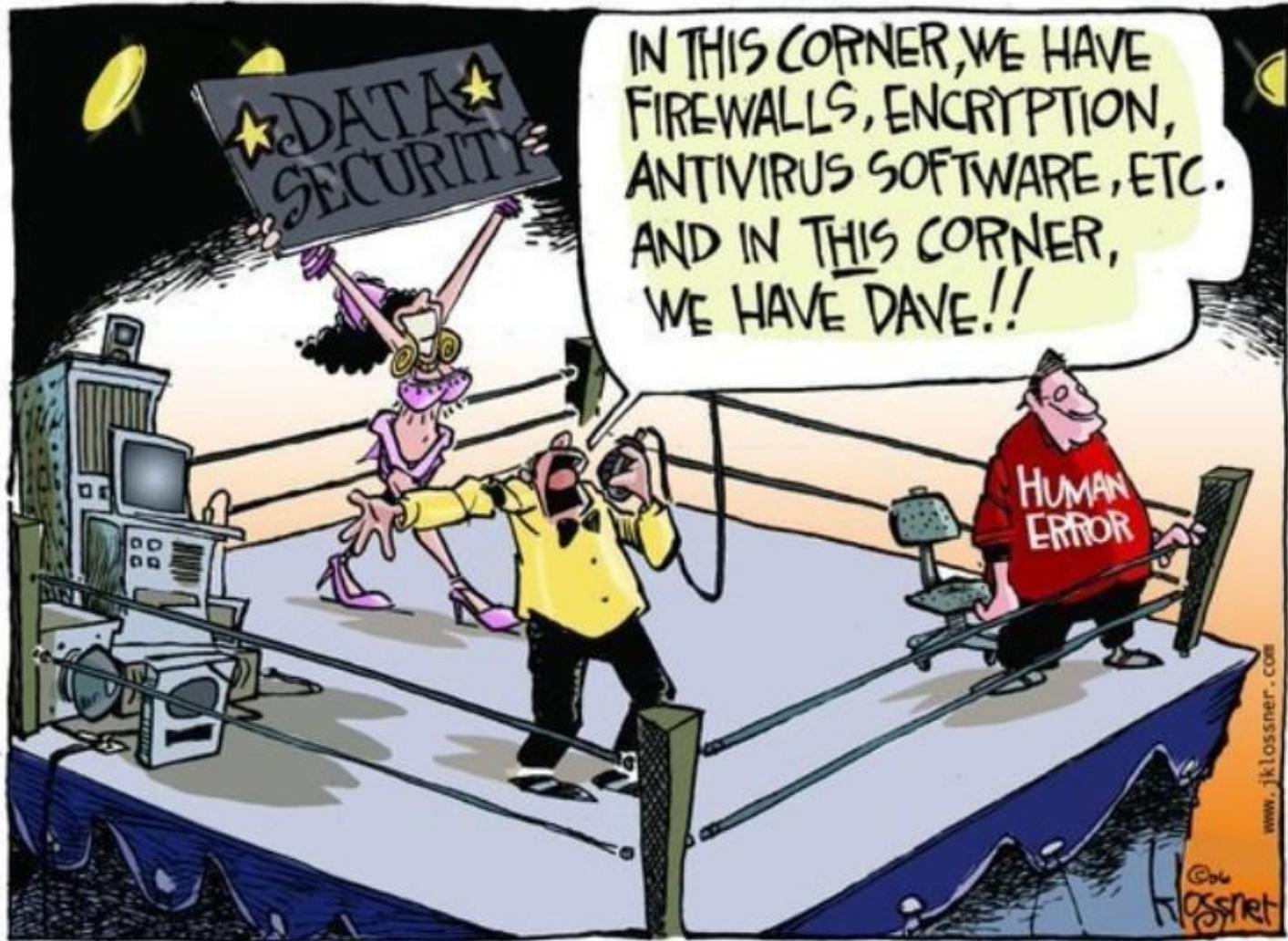
Hoy en día, la adopción tecnológica por parte de la sociedad ha supuesto un desafío para los sectores público y privado que han tenido que involucrarse en los avances actuales para poder satisfacer los nuevos requerimientos de la sociedad y el mercado, debido a que las nuevas tecnologías se integran en su desarrollo con una celeridad cada vez mayor.



#### BCSC colabora con la Diputación Foral de Álava y la Cámara de Comercio de Álava en la concienciación en ciberseguridad en empresas

Uno de los principales objetivos del Centro Vasco de Ciberseguridad (CVCS) es elevar el nivel de medidas en ciberseguridad de la sociedad vasca en todos sus estratos, incluidas las empresas. Perseguindo dicho objetivo, BCSC ha colaborado en la organización de la jornada 'La Ciberseguridad en las empresas alavesas', en colaboración con la Diputación Foral de Álava y la Cámara de Comercio de Álava. Con esta, son ya 17 las jornadas de concienciación impulsadas por el Centro en lo que va de año, con la asistencia de más de 500 profesionales.

[Ver todas las noticias...](#)



copyright 2006 john klossner, [www.jklossner.com](http://www.jklossner.com)

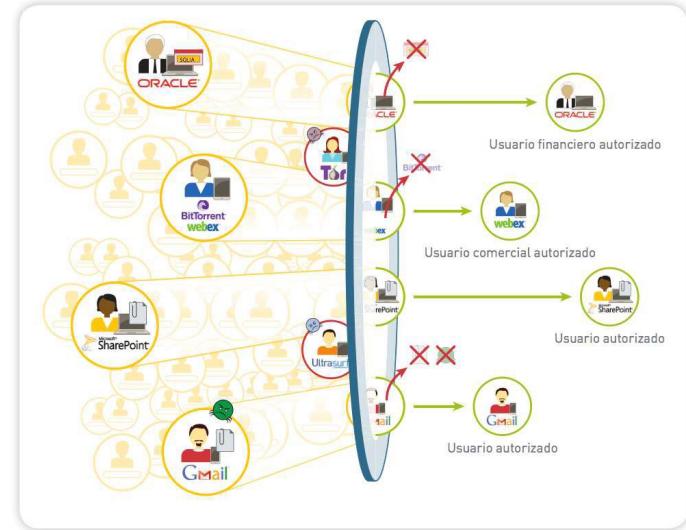
A photograph of the Great Wall of China winding through green, hilly terrain under a dramatic sunset sky.

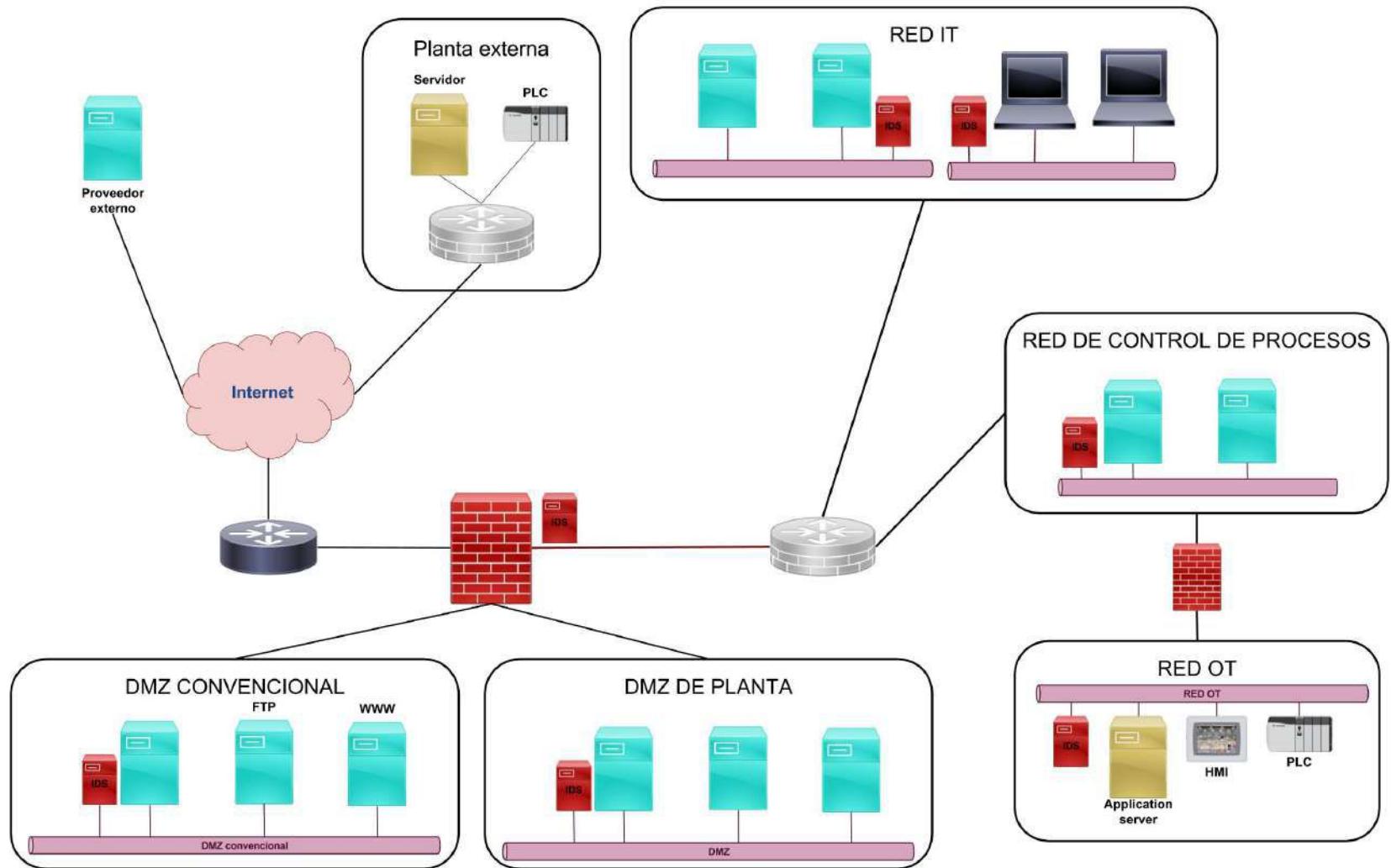
Protección perimetral

# Cyber-Sec... FW:

Tipos de Cortafuegos:

- Cortafuegos de nivel de red.
- Cortafuegos de nivel de aplicación.
- Cortafuegos con inspección de tráfico y detección de intrusiones.
- Cortafuegos de nueva generación.

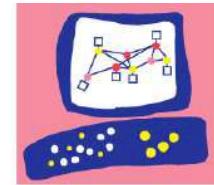




# Cyber-Sec... FW:

Funcionalidades a valorar:

- Filtrado a nivel de aplicación.
- Inspección de contenidos.
- Antivirus.
- Detección de ataques no conocidos.
- Rendimiento con todas las funcionalidades activadas.
- Control de usuarios.
- Limitación de ancho de banda por aplicación o usuario.



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

**FORTINET**®

**SONICWALL**®

## Magic Quadrant

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (May 2016)

Figure 1. Magic Quadrant for Enterprise Network Firewalls



Source: Gartner (October 2018)

## Magic Quadrant

Figure 1. Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)



Source: Gartner (June 2017)

Figure 1. Magic Quadrant for Unified Threat Management (SMB Multifunction Firewalls)



Source: Gartner (September 2018)

Gartner

© Gartner, Inc

Figure 1. Magic Quadrant for Web Application Firewalls

Figure 1. Magic Quadrant for Web Application Firewalls



Source: Gartner (August 2017)



Source: Gartner (August 2018)

© Gartner, Inc

It's yellow, it's ugly, it doesn't match anything,  
but it can save lives.

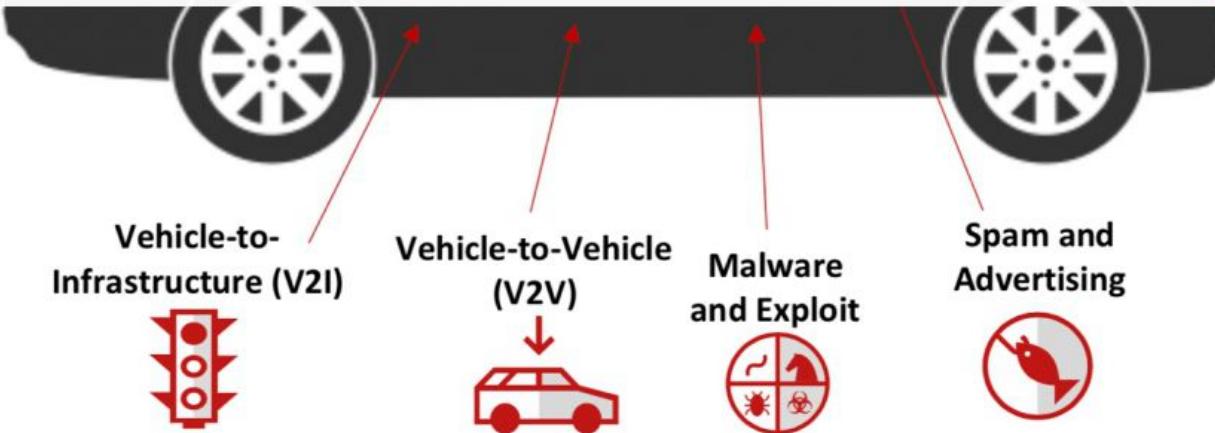
L'IMAGE EST PROTEGÉE PAR LE DROIT D'AUTEUR



Safety vest and reflective triangle will be obligatory in every vehicle. Get equipped now.



**ROAD SAFETY**  
**WE ARE ALL RESPONSIBLE**



La Asociación Mediterránea de Peritos de las Tecnologías de la Información y Comunicación (Aspertic), ha advertido que 189 gasolineras españolas, especialmente las autónomas (sin empleados) se encuentran en grave riesgo en caso de ciberataque debido a las casi nulas medidas de seguridad para impedir que un tercero pueda penetrar en sus sistemas y controlar de forma remota las válvulas de los tanques (684/041283)

Situación: Pendiente de contestación

Fecha límite de contestación: 20/04/2018

▶ Iniciativa



02/03/2018

≡

El PÚBLICO

INICIA SESIÓN UNETE A PÚBLICO

POLÍTICA OPINIÓN MUNDO ECONOMÍA MUJER Y SOCIEDAD MEDIO AMBIENTE PÚBLICO CULTURAS TREMENDING PTV

Hasta 189 gasolineras españolas se pueden hackear fácilmente, denuncian peritos informáticos



EL ESPAÑOL

Ruedas de prensa  
ESTRATEGIA

Un agujero de seguridad haría posible usar 189

000,000,000  
SERIAL... URL...



5 La mala relación de la familia real en Zarzuela es rehabilitada como...

Los videos más vistos



La Voz de Galicia

## «Hackers» éticos de Vigo alertan a la UE de fallos de seguridad en gasolineras

Entre cinco y siete estaciones de servicio en riesgo están ubicadas en Galicia



IoT

# Several Gas Station Design Flaws Allows Attackers to Change the Price and Take Full Control on the Gas Station Remotely

By Priya James - February 28, 2018 0



Reserved CVEs	Description
CVE-2017-14728	Hardcoded Administrator Credentials
CVE-2017-14850	Persistent XSS
CVE-2017-14851	SQL Injection
CVE-2017-14852	Insecure Communication
CVE-2017-14853	Code injection
CVE-2017-14854	Buffer Overflow allows RCE

The screenshot shows a software interface for managing a gas station. On the left, there's a sidebar with buttons for Status, Reports, Wet Stock Mgmt, Circuit Management, Setup, Event Viewer, Admin, and Exit. Below the sidebar is a logo for 'GASBOY'. The main area has tabs for Pumps, Tanks, Devices, and Market Screen. Under the Pumps tab, there are four pump icons labeled 1, 2, 3, and 4, each with fields for USD, gallon, StepMil, No., and Fleet. To the right of the pumps is another set of four pump icons. At the bottom right of this section is a red circular button with a plus sign and the text 'Stop All'. Below the pump controls is a table titled 'Transactions' with columns: Date, Time, Transaction, Receipt, Employee/Vehicle, Oilmeter, Sale (\$), Quantity (gallons), PPV, Fuel Type, Pump, Nozzle, and Density (kg/m³). The table contains several rows of transaction data. At the bottom of the table are navigation buttons for page numbers and a total count of 1-26 (163).

Date	Time	Transaction	Receipt	Employee/Vehicle	Oilmeter	Sale (\$)	Quantity (gallons)	PPV	Fuel Type	Pump	Nozzle	Density (kg/m³)
06/21/17	18:57:31	300115560	115805			25.440	12.121	2.099	Unleaded	2	1	0.000
06/21/17	18:23:31	300115560	115804			54.000	22.050	2.448	Clean Diesel3	1	1	0.000
06/21/17	18:23:30	300115560	115803			162.700	63.000	2.448	Clean Diesel1	1	1	0.000
06/21/17	18:03:30	300115567	115802			21.460	8.013	1.849	Unleaded	1	1	0.000
06/21/17	18:06:55	300115566	115801			8.990	4.565	2.099	Unleaded	2	1	0.000
06/21/17	18:00:32	300115569	115800			234.690	120.401	1.848	Clean Diesel1	1	1	0.000
06/21/17	18:48:07	300115564	115799			83.380	21.798	2.448	Clean Diesel3	1	1	0.000

# La Policía investiga si una gasolinera de 'low cost' pudo ser manipulada para que se pudiera repostar gratis

Ocurrió durante todo el fin de semana. Hasta que dicho surtidor fue precintado, numerosas personas acudieron a llenar el depósito de su coche al correrse la voz

Versión impresa y hemeroteca



**elCorreotv**

DIRECTO

Los propietarios de la gasolinera han presentado una denuncia en la Comisaría de la Policía Nacional de Dos Hermanas y han puesto a disposición de la misma las imágenes de las cámaras de seguridad, para tratar de averiguar si esta 'singular' circunstancia se pudo deber a una avería o a la manipulación intencionada del servicio informático que posibilita el repostaje a cambio del pago con dinero en efectivo o con tarjeta; algo que, según han informado fuentes policiales a este Diario Digital, ya están investigando.

Desde primeras horas de la mañana de este lunes, personal de la gasolinera 'Petroprix', que se encuentra cerrada al público, realiza distintos trabajos para tratar de solucionar la avería y volver a ofrecer el servicio con normalidad.

# PETROPRIX

Terminal de pago en efectivo



638 423 799

Atención al cliente

ESPAÑOL

ENGLISH

Identificar  
Usuario

Bienvenido a PETROPRIX

SE ENCUENTRA EN EL TERMINAL DE PAGO EN EFECTIVO

Empezar



ATENCIÓN! NO DEVUELVE CAMBIO

# PETROPRIX

DIESEL

0.000 €/L

0.000 €/L

GASOLINA 95

24

HORAS  
DESATENDIDA

COM VNC

Upgrade your VNC Server license in order to benefit from premium security features and performance enhancements. Visit the RealVNC web site for more information.





# Gestión y gobierno del riesgo:

1. Gestión del riesgo
  - a. Definición de riesgo
  - b. Marco empresarial
  - c. Importancia en el negocio
  - d. Fases en la gestión del riesgo
  - e. Tipos de riesgo
2. Gobierno corporativo y cumplimiento
  - a. Definición de gobierno
  - b. Objetivos y estrategia de negocio
  - c. Alineación con la estrategia de negocio
  - d. Asegurar y cumplir con la estrategia de negocio
  - e. Marco legal dentro de la empresa
  - f. Prácticas internas en la empresa
  - g. Interacción con terceros



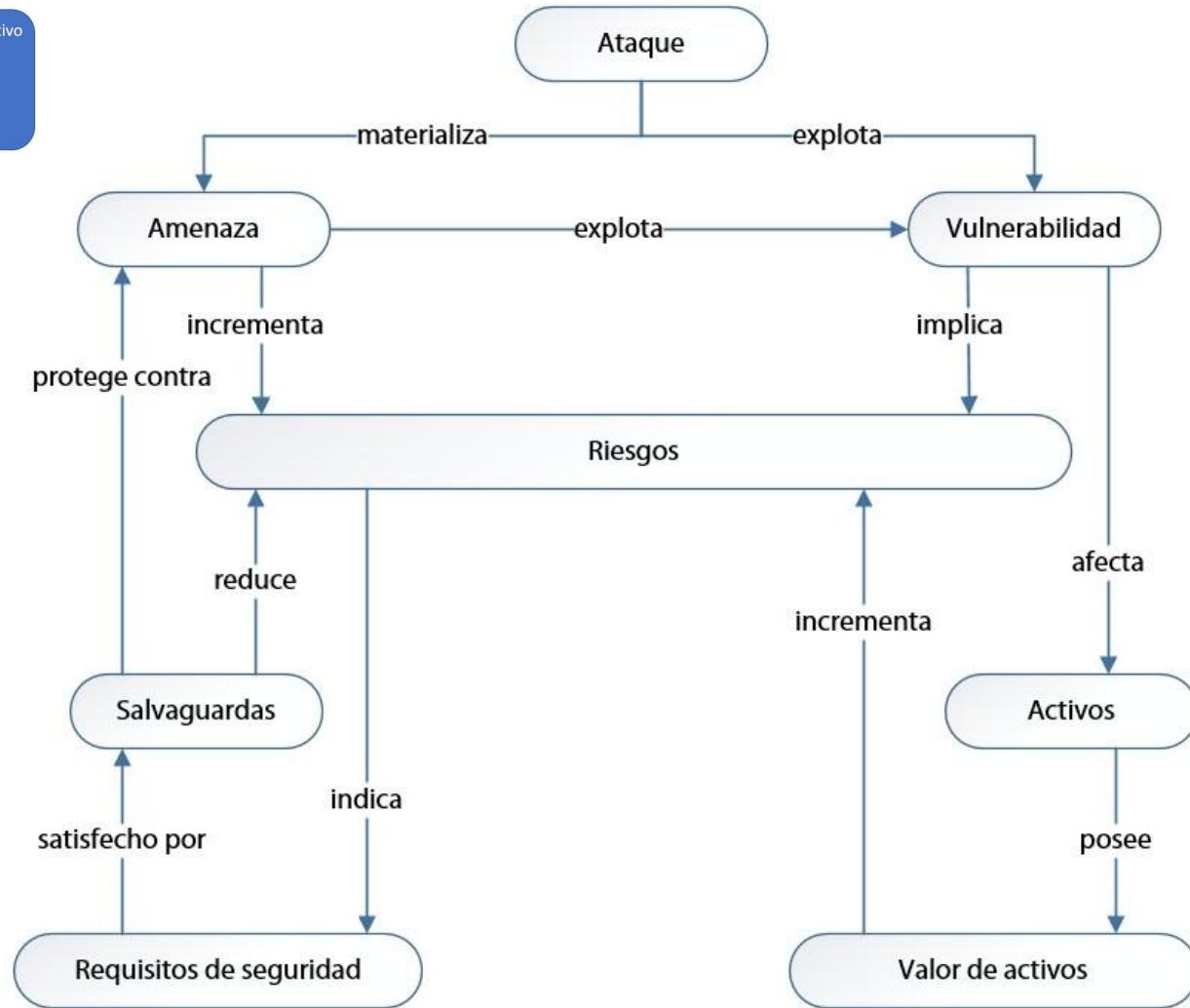
# Gestión del riesgo... Fases análisis:





Origen de la amenaza

Vector de ataque



# Gestión del riesgo... Análisis de riesgo:

## Definición de riesgo:

- Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Los riesgos se calculan en función de la probabilidad de la ocurrencia de un evento y las posibles consecuencias que se cumpla afectando a los activos de la organización.

## Marco empresarial:

- Procesos de seguridad deben actualizarse a los riesgos en constante cambio; Revisión periódica.
- La situación es permanentemente cambiante y los riesgos evolucionan.

# Gestión del riesgo... Análisis de riesgo:

Importancia en el negocio:

- Proceso de identificación, situaciones de exposición ante diferentes riesgos, evaluación del impacto, la magnitud, la frecuencia y consecuencias tras verse afectados.
- Resultado: Informe secreto y confidencial, con la situación actual de peligros que afectan a los activos.
- Objetivo: Definir y aplicar procedimientos, salvaguardas y elaborar planes de contingencia bien definidos para evitar desastres.

Fases en la gestión del riesgo: Identificación de;

- Activos críticos (umbrales de riesgo aceptables. No existe el riesgo cero.)
- Amenazas y Vulnerabilidades
- Evaluación del riesgo.

## PUNTO DE EQUILIBRIO: Costo / Seguridad / Riesgo

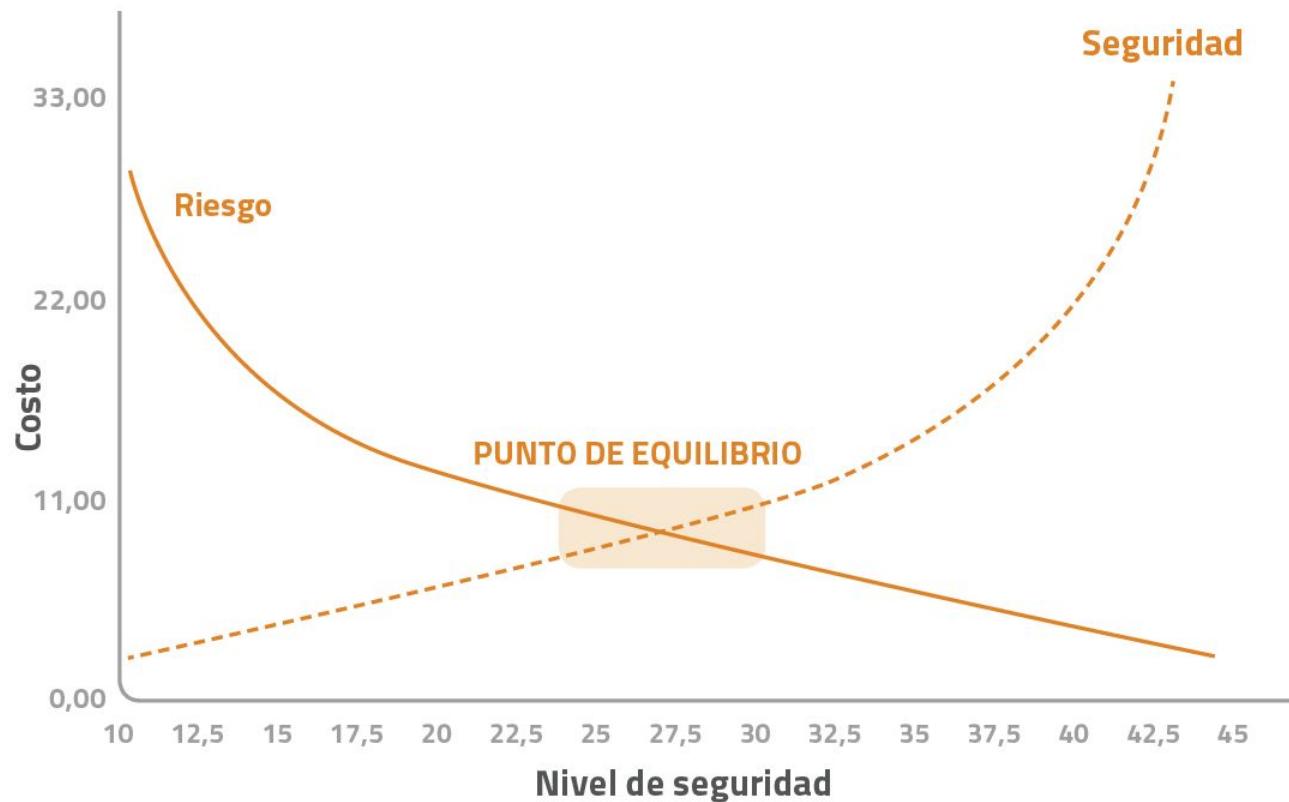


ILUSTRACIÓN 2 - Equilibrio coste sobre las medidas de seguridad

FUENTE: <http://www.segu-info.com.ar/politicas/costos.htm>

# Gestión del riesgo... Análisis de riesgo:

- <https://cybermap.kaspersky.com/es>
- <https://www.fireeye.com/cyber-map/threat-map.html>
- <https://threatmap.checkpoint.com/ThreatPortal/livemap.html>
- <https://threatmap.fortiguard.com/>
- <https://sicherheitstacho.eu/start/main>

Acciones ante el riesgo:

1. Asumir, aceptar el riesgo.
2. Mitigar.
3. Trasladar a un tercero (ej. ciberseguros).
4. Eliminar el riesgo.

Tipos de (análisis de) **riesgo**: Cuantitativo, Cualitativo, (¿Semicuantitativo?)

# Gobierno corporativo y cumplimiento:



# Gobierno corporativo y cumplimiento... Consideraciones:

- Definir y aprobar un plan estratégico de la organización. En este se tendrán que considerar aspectos operativos como el centrado en los sistemas de la organización y sobre Seguridad de la Información.
- Aprobación de documentación interna de la organización: políticas, normas, procedimientos y líneas base.
- Aprobación de material para capacitar y sensibilizar a los empleados en la línea de las necesidades que exige la Dirección.
- Aprobación metodología para la administración de los riesgos de la organización.
- Aprobación de un plan de auditoría que sirva para revisar y asegurar el correcto alineamiento con las legislaciones en vigor y con las políticas y objetivos de la Dirección de la Organización.
- Revisar otros posibles procesos que aseguren el correcto alineamiento con los objetivos de la organización, como pueda la implantación de procesos que aseguren la calidad del dato.

# Gobierno corporativo y cumplimiento... Consideraciones:

- Definición de **gobierno**: gobernanza;
  - Conjunto de políticas (definen el qué), procedimientos (definen el cómo), normas y líneas base que se encargan de definir los planes sobre los que se basa la toma de decisiones importantes de manera global para toda la Organización, impulsadas por la Dirección Ejecutiva y respaldadas por el consejo de administración de la Organización.

# Gobierno corporativo y cumplimiento... Objetivos:

## Objetivos y estrategia de negocio

- Asegurar el cumplimiento de las políticas. Monitorización del cumplimiento.
- Optimizar el uso de los recursos para la protección de la Seguridad de la Información. Planificado.
- Reducir los riesgos por debajo del valor umbral en lo que se refiere la parte operativa del negocio.
- Ofrecer una metodología para la correcta toma de decisiones.
- Ofrecer una metodología y un proceso eficiente para la gestión de incidentes.
- Proporcionar mayor confianza para la relación con proveedores, empleados y clientes.
- Mejorar y proteger la imagen reputacional de la Organización.
- Establecer una serie de actividades que sirvan para proteger la Organización ante actividades críticas para el negocio.
- Establecer una metodología para la continuidad de negocio y la recuperación de procesos en caso de incidente que pueda poner en peligro la actividad de la Organización.



ILUSTRACIÓN 6 - Plan estratégico de una Organización

FUENTE: Concept Consultan

# Gobierno corporativo y cumplimiento... Objetivos:

**Alineación con la estrategia de negocio:** El gobierno de la Seguridad de la Información ofrece y apoya a la dirección en una correcta toma de decisiones. Con el objetivo de definir, implementar y monitorizar un programa de Seguridad de la Información se buscan los siguientes objetivos:

- **Alineación estratégica:** proteger los intereses de la organización implementando aquellos proyectos en materia de seguridad en consonancia y buscando cumplir los objetivos de la Organización.
- **Administrar los riesgos:** definir e implementar una metodología que ayude a mitigar los riesgos identificados y reducir el impacto en los activos.
- Buscar el **retorno de la inversión** y la entrega de valor: optimizar las inversiones y los activos disponibles para llevar a cabo las iniciativas en materia de Seguridad de la Información para la consecución de los objetivos del negocio. Optimización del coste en seguridad.
- Administración de los **recursos disponibles:** utilizar de manera adecuada los recursos disponibles (humanos, tecnológicos, infraestructura, entorno, etc.) de manera eficaz y eficiente.
- **Monitorización del rendimiento:** Definir y reportar distintos indicadores y métricas, capaces de garantizar el buen desempeño de los objetivos de la organización y los distintos procesos críticos.

# Gobierno corporativo y cumplimiento... Estrategia:

Asegurar y cumplir con la estrategia de negocio:

- Modelo de gobierno que pueda reflejar el éxito de objetivos.

Medidores del rendimiento:

- Indicadores: performance **KPI**, risk **KRI**, control **KCI**.
- Métricas
- Datos



# Gobierno corporativo y cumplimiento... Beneficios:

- Incrementa el valor de todas las actividades que desarrolla la Organización.
- Reduce el riesgo que presenta las distintas operativas del negocio elevando la seguridad a niveles aceptables.
- Protege los procesos de negocio frente a cualquier tipo responsabilidad legal y/o penal.
- Optimiza los recursos de la organización en materia de seguridad reduciendo los posibles costes.
- Garantiza la mayor efectividad de las políticas de Seguridad de la información de la Organización.
- Monitoriza los procesos de gestión de riesgos y mejora el proceso de gestión de incidencias relacionadas con Seguridad de la Información.
- Introduce un modelo de roles donde cada persona tiene una responsabilidad definida ante la protección de la información.
- Reduce la posibilidad de que se produzca una violación de la seguridad suponiendo un riesgo para la privacidad de la información.
- Mejora la reputación de la Organización ante la relación con clientes y proveedores.

# Gobierno corporativo y cumplimiento... Legislación:

## Marco legal dentro de la empresa:

- Leyes (obligatoriedad y carácter sancionador)
- Normativas (aplicación voluntaria, reconocimiento, certificación)
- Estándares (documentos y guías de buenas prácticas)
  - <https://www.incibe.es/protege-tu-empresa/herramientas/politicas>
  - <https://www.incibe.es/protege-tu-empresa/kit-conciencionamiento>
  - <https://www.incibe.es/protege-tu-empresa/guias>
  - <https://www.incibe.es/protege-tu-empresa/formacion>
  - <https://www.incibe.es/protege-tu-empresa/que-te-interesa/plan-director-seguridad>

# Gobierno corporativo y cumplimiento... SGSI:

Prácticas Internas en la empresa:

- SGSI:
  - ISO/IEC 27001: especificaciones para los SGSI. Certificable.
  - ISO/IEC 27002: código de buenas prácticas para la implantación del SGSI. Controles (checklist) de la 27001.
  - ISO Guide 72: guía para el desarrollo de sistemas de gestión.
  - BSI - ISO 9000: estándar de calidad.
  - ISO 14000: estándar de gestión medioambiental.
  - ISO 20000: gestión de servicios TI.

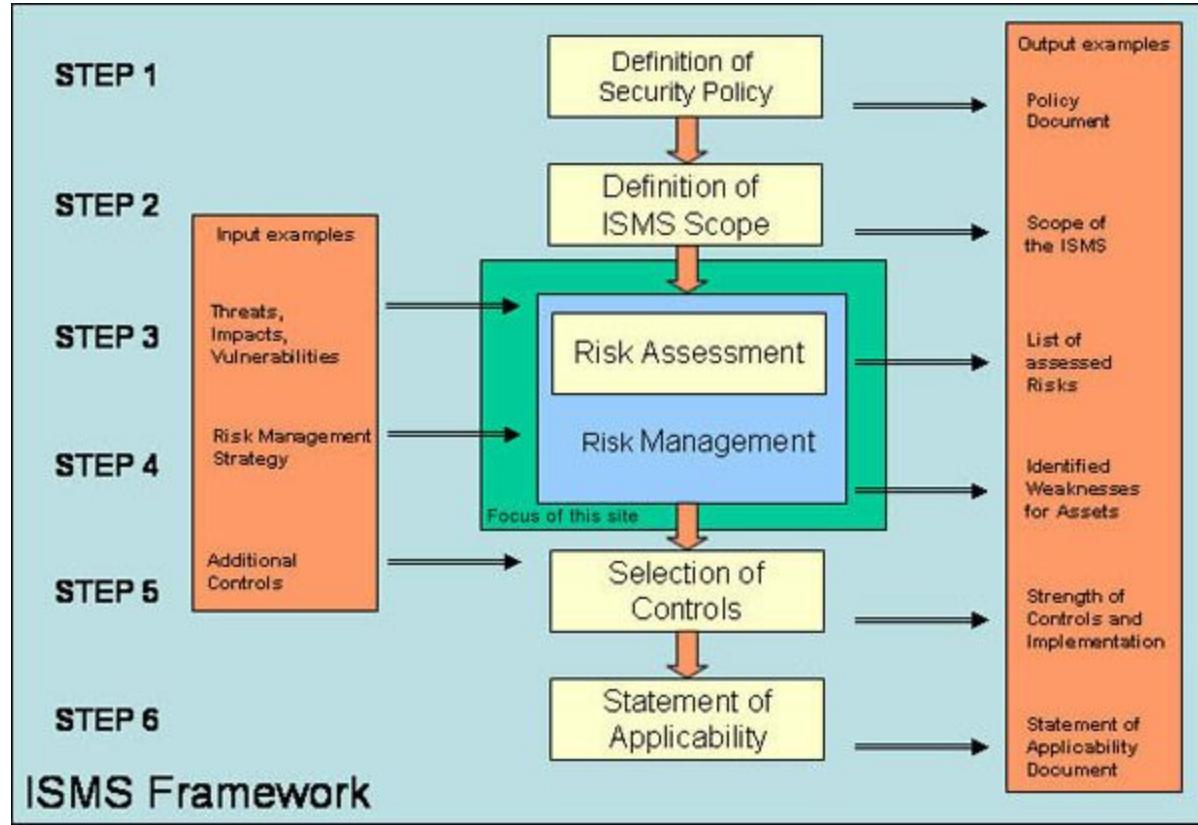
# Gobierno corporativo y cumplimiento... SGSI:

Objetivos:

- Elaborar un marco organizativo donde se establecen los roles y funciones bien definidas.
- Definir los procesos y recursos que son necesarios para lograr los objetivos del negocio.
- Implementar una metodología para la evaluación del rendimiento de los objetivos del negocio, que sirva como punto de partida para establecer un modelo de mejora continua.

# Gobierno corporativo y cumplimiento... SGSI:

- **Política:** se define para demostrar el compromiso de la Dirección de la Organización y los requisitos establecidos para cumplir con los objetivos del negocio.
- **Planificación:** se identifican los elementos críticos, los recursos (humanos, tecnológicos, entorno, proveedores), un marco organizativo y los objetivos a cumplir de manera periódica.
- **Implementación y operación:** se deben indicar las actividades para lograr los objetivos y definir un modelo para gestionar los recursos (materiales y humanos), la documentación. Además de esto, se establece un modelo de comunicación para los distintos estamentos de la Organización, proveedores y clientes.
- **Análisis de rendimiento:** Medición. Definir e implementar una serie de datos que sirvan para alimentar los indicadores clave que sirvan para medir los aspectos clave de la Organización, así como un modelo para gestionar los riesgos que se identifiquen.
- **Mejora continua:** Establecer un modelo de mejora continua que sirva para implementar aquellas acciones que sean necesarias.
- **Revisión por parte de Dirección.**



# Gobierno corporativo y cumplimiento... Consideraciones:

**Interacción con terceros:** SLA, PCI DSS, ...

- Proveedores:
  - Selección, nuevos contratos y consideraciones, modelo de colaboración, renovación de contratos, etc.
    - Adaptación a los requisitos clave del negocio.
    - Comparar servicios competidores.
    - Disponibilidad y capacidad del servicio.
    - Coste y aspectos financieros.
    - Información disponible y actualizada.

# Gestión de la seguridad:

## Gestión de la seguridad:

- Retos dentro del marco empresarial
- Sistemas defensivos: firewalls, IDS, IPS y WAF. (Netfilter iptables/ selinux)
- Monitorización, vigilancia digital y fuentes OSINT
- Vulnerabilidad
- Correlación de logs

# Gestión de la seguridad... Retos:

Retos dentro del marco empresarial:

- Diseñar una política de seguridad, que esté correctamente alineada con los objetivos de la Organización, teniendo en cuenta la participación de empleados, proveedores y clientes.
- Asegurar que se van a cumplir los niveles de servicio que se contemplan en los SLA's.
- Minimizar los riesgos que amenacen a los procesos y actividades críticas del negocio y que pongan en riesgo la actividad de la Organización.
- Conseguir implantar una cultura de la seguridad dentro de los distintos niveles de la Organización.
- Priorizar las oportunidades empresariales que ofrece el mercado sin perder la necesidad existente de preservar la Seguridad de la Información.
- Hacer entender al personal clave las necesidades del negocio que permitan prestar unos servicios que aseguren la correcta gestión de la información.
- Gestionar la seguridad de manera proactiva detectando los riesgos de seguridad que puedan poner en riesgo las actividades de la Organización.

# Gestión de la seguridad... Defensa activa:

Sistemas defensivos:

- Firewall (Hardware/Software. Con estado/ Sin estado)
- IDS (Detección e informe en su propio formato)
- IPS (Prevención, se sitúa en medio, evalúa y procesa para cortar el ataque o dejar pasar el paquete)
- WAF (A nivel de aplicación, también para bases de datos)

**Defensa en profundidad:** Seguridad interna por capas y niveles. (Perimetral, red interna, segmentos de red, host, Servidores (físicos y virtualizados), Aplicación.)





# Gestión de la seguridad... OSINT:

Monitorización, servicios contratados de **vigilancia digital** (marketing) y fuentes OSINT

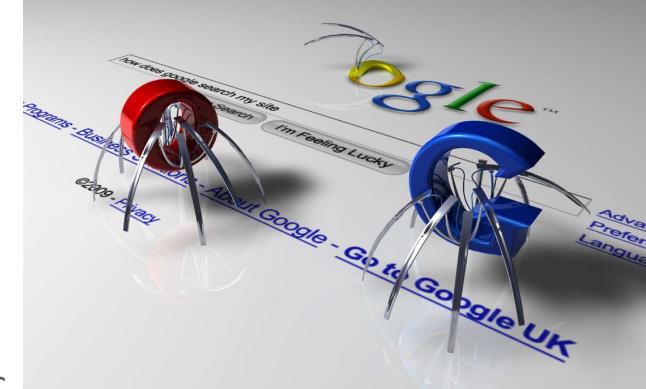
<https://www.sombrero-blanco.com/ciberseguridad/motores-de-busqueda-para-tus-actividades-hackers/>

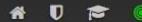
Inteligencia, fuentes de datos:

- HUMINT: Fuentes de información humana (human intelligent).
- SIGINT: Señales de sensores e IoT.
- GEOINT: Informaciones que provienen de satélites (Gespacial Intelligence).
- OSINT: Fuentes de información de acceso libre, gratuitas y desclasificadas (Open Source Intelligence).

# Gestión de la seguridad... OSINT:

- Anticipar acontecimientos, ataques DDoS, atentados terroristas, etc.
- Analizar robos y fugas de información de empresas, gobiernos, etc.
- Investigar personas, organizaciones, objetivos, eventos, etc.
- Monitorizar lo que se habla en redes sociales, foros, IRCs, chats y blogs. Complejidad del lenguaje natural: Análisis de sentimientos (ironía, sarcasmo, etc).
- Analizar relaciones entre personas, empresas, asociaciones, partidos, etc.
- Detectar fallos de configuración que impliquen la exposición de información.
- Monitorizar e investigar páginas fraudulentas y phishing.
- Monitorizar tendencias sobre lo que se habla en Internet de una organización, producto, persona, etc.





dns recon & research, find & lookup dns records

Loading...

DNSdumpster.com is a FREE domain research tool that can discover hosts related to a domain. Finding visible hosts from the attackers perspective is an important part of the security assessment process.

this is a [HackerTarget.com](#) project

Open Source Intelligence for Networks



#### Attack

The ability to quickly identify the attack surface is essential. Whether you are penetration testing or chasing bug bounties.



#### Defend

Network defenders benefit from passive reconnaissance in a number of ways. With analysis informing information security strategy.

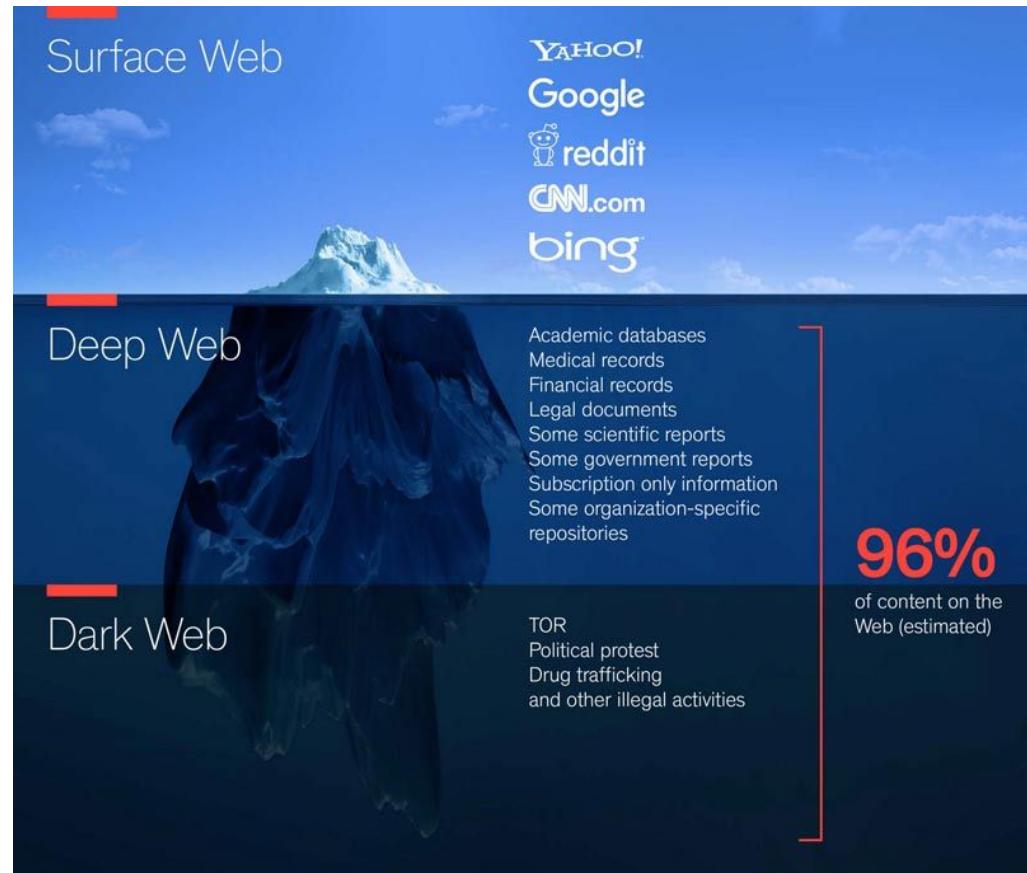


#### Learn

Understanding network based OSINT helps information technologists to better operate, assess and manage the network.

# Gestión de la seguridad... Deep Web:

- Surface Web
- Deep Web
- Dark Web.
  - http tunelado que requiere de software específico.



# Gestión de la seguridad... Vigilancia Digital:

Definir, implementar y monitorizar un sistema de vigilancia digital (Inteligencias artificiales y analistas) proporciona las siguientes ventajas:

- **Análisis de las opiniones** de los clientes, empleados o colaboradores: el proceso de vigilancia digital agrupa las ocurrencias que los usuarios vierten sobre la Organización. A partir de ellas, podrán ser analizadas para mejorar ciertos aspectos relacionadas con las actividades de la Organización.
- **Responder ante una ocurrencia negativa**: analizar las opiniones negativas va a permitir a la Organización actuar para responder al usuario, información práctica, links de ayuda, etc. Es habitual que para este punto existan cuentas en redes sociales gestionadas por la propia Organización.
- **Crear estrategia de comunicación**: el análisis de todos los comentarios que son recogidos a partir de la plataforma de vigilancia digital va a permitir crear una estrategia de comunicación para mejorar el posicionamiento de la Organización ante la opinión pública.

# Gestión de la seguridad... Monitorización:

Afrontar, detectar y resolver los nuevos retos:

- Fraude online (phishing bancarios de mi propia entidad, etc.)
- Seguridad Informática
- Análisis de la Deep Web
- Análisis de posibles ciberataques
- Análisis de los ciberataques a sitios web, estudiar el *modus operandi*, etc.

# Gestión de la seguridad... Vulnerabilidad:

Vulnerabilidad: Fallo o debilidad en el sistema: la definición, diseño, la implementación, la operación o la gestión de un sistema, que puede ser atacado con motivo de violar la política de seguridad del sistema.

- errores en la implementación del servidor
- soporte inadecuado
- carencias en el SO
- inexperiencia del personal
- ausencia de protección de los protocolos de comunicación
- etc.



# Gestión de la seguridad... Vulnerabilidad:

- Procedimiento, gestión y explotación:
  - SOC, CERT (certifiable), CSIRT.
  - <https://www.first.org/members/map#country%3AES>
- Monitorización y registro:
  - alerta temprana.



<b>Team</b>	<b>Official Team Name</b>
BBVA CERT	BBVA CERT
BCSC	Basque CyberSecurity Centre
CaixaBank Team	CAIXABANK TEAM
CCN-CERT	CCN-CERT (Spanish Government National Cryptologic Center - Computer Security Incident Response Team)
CERT OESIA	CERT OESIA
CERTSI	CERT de Seguridad e Industria
CESISCAT-CERT	Information Security Centre of Catalonia
CSIRT-CV	Centro de Seguridad TIC de la Comunitat Valenciana
esCERT-UPC	CERT of the Polytechnic University of Catalonia
eSOC Ingenia	eSOC Ingenia
ESP DEF CERT	CERT - Mando Conjunto de Ciberdefensa
EULEN-CCSI-CERT	EULEN Seguridad-CCSI-CERT
everis CERT	everis CERT
InnoTec Entelgy CSIRT	InnoTec Entelgy CSIRT
ITS-CERT	ITS Industrial Cybersecurity CERT
MAPFRE-CCG-CERT	Equipo de Respuesta a Incidentes de Seguridad de la Información del CCG de MAPFRE
Minsait CSIRT	Minsait CSIRT
NestleSOC	Nestle Cyber Security Operations Center
PROSEGUR CERT	PROSEGUR CERT
RedIRIS	RedIRIS
RENFE	RENFE-Operadora
S2 Grupo CERT	S2 Grupo CERT
S21sec CERT	S21sec CERT
SIA-CEC CERT	SIA-CEC CERT
Telefonica-CSIRT	Telefonica CSIRT

# Gestión de la seguridad... Vulnerabilidad:

OWASP: [https://www.owasp.org/index.php/Category:OWASP\\_Top\\_Ten\\_Project](https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

- Inyección SQL, OS, LDAP.
- Pérdida de autenticación y gestión de sesiones.
- Secuencia de comandos en sitios cruzados (XSS).
- Referencia directa insegura a objetos
- Configuración de seguridad incorrecta
- Exposición de datos sensibles
- Ausencia de control de acceso a las funciones
- Falsificación de peticiones en sitios cruzados (CSRF)
- Uso de componentes con vulnerabilidades conocidas
- Redirecciones y reenvíos no validados

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Inyección	→	A1:2017 – Inyección
A2 – Pérdida de Autenticación y Gestión de Sesiones	→	A2:2017 – Pérdida de Autenticación y Gestión de Sesiones
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	→	A3:2017 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos [Unido+A7]	U	A4:2017 – Entidad Externa de XML (XXE) [NUEVO]
A5 – Configuración de Seguridad Incorrecta	→	A5:2017 – Pérdida de Control de Acceso [Unido]
A6 – Exposición de Datos Sensibles	↗	A6:2017 – Configuración de Seguridad Incorrecta
A7 – Ausencia de Control de Acceso a las Funciones [Unido+A4]	U	A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	✗	A8:2017 – Deserialización Insegura [NUEVO, Comunidad]
A9 – Uso de Componentes con Vulnerabilidades Conocidas	→	A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	✗	A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]

<b>A1:2017</b> <b>Inyección</b>	Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.
<b>A2:2017</b> <b>Pérdida de Autenticación</b>	Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).
<b>A3:201</b> <b>Exposición de datos sensibles</b>	Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.
<b>A4:2017</b> <b>Entidades Externas XML (XXE)</b>	Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).
<b>A5:2017</b> <b>Pérdida de Control de Acceso</b>	Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc.
<b>A6:2017</b> <b>Configuración de Seguridad Incorrecta</b>	La configuración de seguridad incorrecta es un problema muy común y se debe en parte a establecer la configuración de forma manual, <i>ad hoc</i> o por omisión (o directamente por la falta de configuración). Son ejemplos: S3 buckets abiertos, cabeceras HTTP mal configuradas, mensajes de error con contenido sensible, falta de parches y actualizaciones, frameworks, dependencias y componentes desactualizados, etc.
<b>A7:2017</b> <b>Secuencia de Comandos en Sitios Cruzados (XSS)</b>	Los XSS ocurren cuando una aplicación toma datos no confiables y los envía al navegador web sin una validación y codificación apropiada; o actualiza una página web existente con datos suministrados por el usuario utilizando una API que ejecuta JavaScript en el navegador. Permiten ejecutar comandos en el navegador de la víctima y el atacante puede secuestrar una sesión, modificar ( <i>defacement</i> ) los sitios web, o redireccionar al usuario hacia un sitio malicioso.
<b>A8:2017</b> <b>Deserialización Insegura</b>	Estos defectos ocurren cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones o elevar sus privilegios de ejecución. En el peor de los casos, la deserialización insegura puede conducir a la ejecución remota de código en el servidor.
<b>A9:2017</b> <b>Componentes con vulnerabilidades conocidas</b>	Los componentes como bibliotecas, frameworks y otros módulos se ejecutan con los mismos privilegios que la aplicación. Si se explota un componente vulnerable, el ataque puede provocar una pérdida de datos o tomar el control del servidor. Las aplicaciones y API que utilizan componentes con vulnerabilidades conocidas pueden debilitar las defensas de las aplicaciones y permitir diversos ataques e impactos.
<b>A10:2017</b> <b>Registro y Monitoreo Insuficientes</b>	El registro y monitoreo insuficiente, junto a la falta de respuesta ante incidentes permiten a los atacantes mantener el ataque en el tiempo, pivotear a otros sistemas y manipular, extraer o destruir datos. Los estudios muestran que el tiempo de detección de una brecha de seguridad es mayor a 200 días, siendo típicamente detectado por terceros en lugar de por procesos internos

## Resumen de factores de Riesgo del Top 10

La siguiente tabla presenta un resumen del Top 10 y los factores de riesgo que hemos asignado a cada uno de ellos.

Estos factores fueron determinados basándose en las estadísticas disponibles y la experiencia del equipo del OWASP Top 10. Para entender estos riesgos en una aplicación en particular u organización, usted debe considerar sus propios agentes de amenaza e impactos de negocio específicos. Incluso las vulnerabilidades graves de software podrían no representar un riesgo serio si no hay agentes de amenaza en posición para ejecutar el ataque necesario, o el impacto al negocio es insignificante para los activos involucrados.

Riesgo	Agentes de Amenaza	Vectores de Ataque		Debilidades de Seguridad		Impacto		Puntuación
		Explotabilidad	Prevalencia	Detectabilidad	Técnico	Negocio		
A1: 2017- Inyección	Específico de la Aplicación	FACIL: 3	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	8,0	
A2: 2017 - Pérdida de Autenticación	Específico de la Aplicación	FACIL: 3	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0	
A3: 2017 - Exposición de Datos Sensibles	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	7,0	
A4: 2017 - Entidad Externa de XML (XXE)	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	FACIL: 3	GRAVE: 3	Específico de la Aplicación	7,0	
A5: 2017 - Pérdida de Control de Acceso	Específico de la Aplicación	PROMEDIO: 2	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	6,0	
A6: 2017 - Configuración de Seguridad Incorrecta	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0	
A7: 2017 - Secuencia de Comandos en Sitios Cruzados (XSS)	Específico de la Aplicación	FACIL: 3	DIFUNDIDO: 3	FACIL: 3	MODERADO: 2	Específico de la Aplicación	6,0	
A8: 2017 - Deserialización Insegura	Específico de la Aplicación	DIFÍCIL: 1	COMUN: 2	PROMEDIO: 2	GRAVE: 3	Específico de la Aplicación	5,0	
A9: 2017 - Componentes con Vulnerabilidades Conocidas	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	PROMEDIO: 2	MODERADO: 2	Específico de la Aplicación	4,7	
A10: 2017 - Registro y Monitoreo Insuficientes	Específico de la Aplicación	PROMEDIO: 2	DIFUNDIDO: 3	DIFÍCIL: 1	MODERADO: 2	Específico de la Aplicación	4,0	



Common Vulnerabilities and Exposures

CVE List

CNIAs

Board

About

News & Blog

NVD

Go to for:

[CVSS Scores](#)

[CPE Info](#)

[Advanced Search](#)

Search CVE List

Download CVE

Data Feeds

Request CVE IDs

Update a CVE Entry

TOTAL CVE Entries: **110818**

CVE® is a [list](#) of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities.

CVE Entries are used in numerous cybersecurity [products and services](#) from around the world, including the U.S. National Vulnerability Database ([NVD](#)).

## CNA Participation Growing Worldwide



### CVE Numbering Authorities (CNAs)

Totals CNAs: [93](#) | Total Countries: [16](#)

CNAs include vendors and projects, vulnerability researchers, national and industry CERTs, and bug bounty programs.

CNAs are how the [CVE List](#) is built. Every [CVE Entry](#) added to the list is assigned by a CNA.

[How to Become a CNA >>](#)

## Latest CVE News

- [Minutes from CVE Board Teleconference Meeting on November 28 Now Available](#)
- [MongoDB Added as CVE Numbering Authority \(CNA\)](#)
- [New CVE Board Member from DHS](#)

[More >>](#)

## CVE Blog

### A Look at the CVE and CVSS Relationship

We've received a few questions recently about the [Common Vulnerability Scoring System \(CVSS\)](#) and vulnerability severity scoring, so as a reminder, CVSS is a separate program from CVE.

CVE is a [list](#) of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE does not provide severity scoring or prioritization ratings for software vulnerabilities.

However, while separate, the [CVSS](#) standard can be used to score the severity of CVE Entries.

[More >>](#)

## Newest CVE Entries

[Newest CVE IDs by @CVEnew](#)

[Follow @CVEnew >>](#)



Main Menu

About Us  
White Papers  
Security Advisories  
CERT Top Stories  
CERT Top Stories - 24h  
Latest News  
Big Screen Map  
Breaking News  
Advanced Search  
News about CERTs  
Hall Of Fame  
Vacancies at CERT-EU

Product Vulnerabilities +

Vulnerabilities +

Threats and Incidents +

Hacking/techniques +

Latest News About - Ongoing threats

Show/hide duplicate news articles.

1 2 3 4 5 6 7 8 9 10 > +10 🔍

Top Stories

- Netflix bows to the Saudi Kingdom by pulling critical satire episode: Comedy is dead
- Articles : 19 | Last update : Jan 3, 2019 12:55:00 PM | Start : Jan 1, 2019 6:39:00 PM | Sources : 15 | Peak : 1 | Current rank : 1
- Vietnam's draconian cybersecurity bill comes into effect, SE Asia News & Top Stories - The Straits Times
- Articles : 20 | Last update : Jan 3, 2019 1:51:00 PM | Start : Jan 1, 2019 9:48:00 AM | Sources : 14 | Peak : 2 | Current rank : 2
- HHS Publishes Guide to Cybersecurity Best Practices
- Articles : 14 | Last update : Jan 3, 2019 12:02:00 PM | Start : Dec 31, 2018 7:05:00 PM | Sources : 9 | Peak : 3 | Current rank : 3
- Stop the Presses: Don't Rush Tribune Ransomware Attribution
- Articles : 12 | Last update : Jan 3, 2019 10:19:00 AM | Start : Dec 31, 2018 6:05:00 PM | Sources : 10 | Peak : 2 | Current rank : 4
- Major US newspapers suffer malware attack; printing & delivery affected
- Articles : 111 | Last update : Jan 3, 2019 12:05:00 PM | Start : Dec 30, 2018 12:19:00 AM | Sources : 57 | Peak : 5 | Current rank : 5
- USB Type-C authentication program launches to protect against hardware hacks
- Articles : 12 | Last update : Jan 3, 2019 11:41:00 AM | Start : Jan 2, 2019 5:30:00 PM | Sources : 11 | Peak : 8 | Current rank : 6
- It's Great to Go Straight
- Articles : 9 | Last update : Jan 2, 2019 1:11:00 PM | Start : Jan 2, 2019 11:54:00 AM | Sources : 9 | Peak : 6 | Current rank : 7
- EU launches Bug Bounty program for 14 free open-source products
- Articles : 19 | Last update : Jan 3, 2019 9:32:00 AM | Start : Dec 28, 2018 2:48:00 AM | Sources : 14 | Peak : 4 | Current rank : 8
- PewDiePie mains results in hacking campaign against Chromecast, Google Home devices
- Articles : 11 | Last update : Jan 3, 2019 12:32:00 PM | Start : Jan 2, 2019 9:29:00 PM | Sources : 11 | Peak : 9 | Current rank : 9
- Attacks Against Critical Infrastructure Poised to Reshape Cyber Landscape (SecurityWeek)
- Articles : 5 | Last update : Jan 3, 2019 1:31:00 PM | Start : Jan 2, 2019 6:38:00 PM | Sources : 5 | Peak : 12 | Current rank : 10

Latest articles

Afsluisterstation geheime dienst moet wijken voor 5G in Nederland

OneMoreThing Thursday, January 3, 2019 3:22:00 PM CET | info [en] [other]

Niets staat de uitrol van 5G in Nederland meer in de weg, want het laatste bezwaarpunt is net voor kerst weggenomen. Het ging om het afsluisterstation van de Nederlandse inlichtingendiensten in Burum (Friesland). Dat werkt op dezelfde frequentie als het toekomstige 5G-netwerk....



Microsoft's Top 3 Cybersecurity Concerns for 2019

govinfosecurity Thursday, January 3, 2019 3:18:00 PM CET | info [other]

With an operating system that's used by 90 percent of Fortune 500 companies, Microsoft closely monitors cyberattack trends. It spends over \$1 billion a year on mitigating threats, says Joram Borenstein, general manager of Microsoft's Cybersecurity Solutions Group, who discusses his top three concerns for 2019....



Articles published more than 10 minutes ago

Cyber Security Roundup for December 2018

securityboulevard Thursday, January 3, 2019 3:12:00 PM CET | info [other]

The final Cyber Security Roundup of 2018 concludes reports of major data breaches, serious software vulnerabilities and evolving cyber threats, so pretty much like the previous 11 months of the year, had their accounts compromised, after the company reportedly didn't secure their internet connected databases properly....

Info

This website is managed by CERT-EU. Find out more about us.

For questions or comments, please contact us at:  
email: [cert-eu@ec.europa.eu](mailto:cert-eu@ec.europa.eu)  
PGP Fingerprint: D894 7318 0495 62AB 9DE8  
41DC B9F8 FCC1 B607 5A8B  
Emergency phone: +3222390005

Tools

Thursday, January 3, 2019  
3:19:00 PM CET



RSS



Facebook



subscribe | manage



current page | all pages



info | definition

Available on the ANDROID APP ON

Languages

Select top stories in other languages.

ar cs da de el en  
es et fa fi fr he  
hr hu id it ja ko  
it lv mk mt nl no  
pl pt ro ru sk sl  
sv th tr uk zh  
all

Interface: en - English

Legend

Most reported countries (24h)

## Current FIRST SIGs

### Academic Security SIG

Space for discussion in order to reflect on our collective experiences, focus on current challenges and envision strategies on how we could work together to improve security in academic environments.

### Big Data SIG

Incident Detection and Response at Scale.

### Capture the Flag SIG

Designs, develops, and conducts security challenge and competition exercises for the FIRST.org community.

### CVSS SIG: Common Vulnerability Scoring System

For a global approach towards scoring metrics for vulnerabilities.

### Cyber Threat Intelligence SIG

To define Threat Intelligence in the commercial space.

### Ethics SIG

The Ethics SIG seeks to further the professionalization of the FIRST Community and improve the global understanding of SIRTs through the development of an ethical code for FIRST Members.

### ICS SIG: Industrial Control Systems

In ICS-SIG we bring together expertise from several sectors to create processes, best practices and incident response support recommendations and package useful open source tools for the ICS environments.

## Events at spotlight



## FIRST is the global Forum of Incident Response and Security Teams

FIRST is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents reactive as well as proactive.

FIRST brings together a variety of computer security incident response teams from government, commercial, and educational organizations. FIRST aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

Apart from the trust network that FIRST forms in the global incident response community, FIRST also provides value added services. Some of these are:

- access to up-to-date best practice documents
- technical colloquia for security experts
- hands-on classes
- annual incident response conference
- publications and web services
- special interest groups

Currently FIRST has more than 400 members, spread over Africa, the Americas, Asia, Europe and Oceania.

## What's New

FIRST is calling for nominations for the Incident Response Hall of Fame

Members who would like to nominate a qualified individual or team should complete the form by April 2019 here: <https://first.org/hof/>

(Fri, 07 Dec 2018 19:20 -0000)

## 2019 Event Calendar

The 2019 event calendar has been updated. We have several events with open registration so please update your calendars and register today!

(Fri, 07 Dec 2018 10:00 -0000)

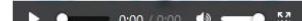
## Call for Trainers!

Would you like to find a way to give back to FIRST and the incident response community? Sign-up on our first-trainers list to be notified of opportunities to travel the world and share your expertise. FIRST will provide the materials and travel if you provide your time and knowledge. Contact [first-sec@first.org](mailto:first-sec@first.org) for more details.

(Fri, 07 Dec 2018 09:00 -0000)

## What is FIRST to you?

What is FIRST ?



# Gestión de la seguridad... LOGs:



Correlación de logs:

- SIEM: Centralización de logs y eventos.
- CERT / SOC.



# Respuesta a incidentes... Incident Response:

- Introducción
- Definición de incidente de seguridad
- Procedimientos de respuesta ante incidentes
- Equipos de respuesta ante incidentes
- Perfil y herramientas del atacante
- Análisis forense de un incidente de seguridad

# Respuesta a incidentes... Incident Response:

- Introducción:
  - Ataques no anticipados.
  - Pérdidas de información.
  - Robo de datos.
  - Cualquier evento adverso que ocurra como resultado de controles fallidos, inexistentes o cualquier corte en la actividad de los procesos de la Organización.
- DFIR (digital forensics Incident Response)
  - - *“Si cree usted que la educación es cara, pruebe con la ignorancia”*
    - - *“Si piensas que la seguridad es cara, prueba con la respuesta a incidentes”*

# Respuesta a incidentes... Objetivos:

- Detectar los incidentes que impactan en la actividad de la Organización de manera ágil. Registro de entrada.
- Realizar un análisis del incidente de seguridad para verificar el porqué de lo ocurrido.
- Reducir y minimizar las consecuencias del incidente de seguridad.
- Restaurar los servicios que puedan haber sufrido una parada en su actividad.
- Gestionar con los departamentos implicados la incidencia de seguridad.
- Documentar cuales han sido las causas que ha producido el incidente.
- Implementar aquellas mejoras que se hayan identificado a lo largo del proceso de resolución del incidente.
- Realizar un informe con la historia del incidente explicando todos los pasos desarrollados para resolverlo. Lecciones aprendidas. Actividad post-incidente.



# Respuesta a incidentes... Incident Response:

Definición de **incidente** de seguridad:

- **CERT:** Amenaza inminente a la Política de Seguridad de la Información tanto de manera directa como indirecta o como un intento de acceso uso, divulgación, modificación o destrucción no autorizada de información que hace de impedimento a la operación normal de las redes, sistemas o recursos informáticos.
- **ISO/IEC 27005:** Una serie de eventos de Seguridad de la Información que son indeseados o inesperados que pueden poner en riesgo o comprometer las operativas del negocio y amenazan a la Seguridad de la Información.



# Respuesta a incidentes... Incident Response:

Tipos de **incidentes** de seguridad:

- Acceso no autorizado a recursos protegidos.
- Robo de contraseñas o información confidencial; Ej. Leak público.
- Prácticas de ingeniería social.
- Utilizar las vulnerabilidades en el proceso de autenticación para acceder a los sistemas; Parcheo y actualización.
- Acceso o uso indebido de la información almacenada sin el permiso del propietario.
- Vulnerar los servicios informáticos internos o externos de la información.
- Alterar el código fuente de las aplicaciones de la Organización; Ej. Insider: Alta gravedad, requiere de forense.
- Introducir código malicioso dentro de la infraestructura tecnológica de la Organización, mediante virus, troyanos, gusanos o malware; Aislar el malware, investigar y entender su funcionamiento.
- Ataques de denegación de servicio que ocasionan paradas en el servicio de la Organización y que impiden cumplir los tiempos de respuesta y acuerdos de nivel de servicio estipulados.
- Cualquier situación externa que pueda comprometer la Seguridad de la Organización, como pueda ser la quiebra de un proveedor o una epidemia de gripe o la intoxicación alimenticia en el comedor de la Organización.

# Respuesta a incidentes... Incident Response:

## Procedimientos de respuesta ante incidentes

- No existe la seguridad al 100%. No existen garantías que aun implantando unos controles muy maduros y completos esto impida la ocurrencia de incidentes que perjudiquen la operativa de la Organización. Definir, mantener y mejorar el proceso de gestión de incidentes permite a la Organización continuar con sus operaciones en caso de interrupción y superar la violación a la seguridad de los sistemas de información.

## Factores que agravan la ausencia de un proceso maduro de gestión de incidentes:

- El aumento de situaciones en las que la Organización sufre pérdidas ante la ocurrencia de incidentes de seguridad.
- El aumento de las vulnerabilidades en los sistemas y el software implantado en la Organización.
- El aumento de atacantes que buscan un beneficio económico cuando explotan una vulnerabilidad.
- El aumento de los distintos departamentos que exigen una adecuada gestión de incidentes.

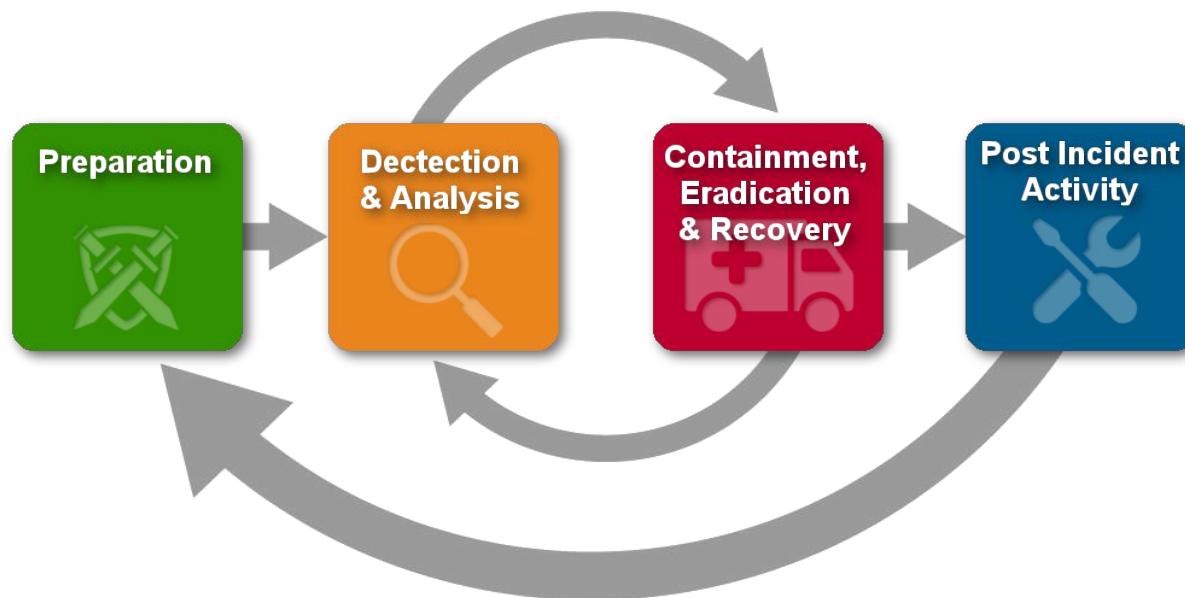
# Respuesta a incidentes... Incident Response:

Una buena gestión de incidentes: Capacidad suficiente para la **detección** y la **monitorización** de los incidentes, con criterios de gravedad bien definidos, una buena gestión de la comunicación a los distintos estamentos de la Organización y una buena cultura que permita que los empleados puedan gestionar de manera adecuada los incidentes.

- Foco en la detección.
- Proteger de manera adecuada los activos de la Organización.
- Contar con planes eficaces de respuesta ante incidentes que estén en conocimiento de todos los niveles de la Organización.
- Permitir resolver y documentar el proceso de gestión de incidencias.
- Disponer de un proceso de mejora continua que permite aprender de aquellos defectos identificados en la gestión de incidentes.
- Garantizar la operativa del negocio, tanto a proveedores como a clientes.

# Respuesta a incidentes... Incident Response:

Equipos de respuesta rápida ante incidentes (CERT, IRT, etc.)



# Respuesta a incidentes... CERT:



**CERT (CSIRT):** Equipos de respuesta ante incidentes: medidas preventivas y reactivas;

- Dar soporte a los empleados, clientes o proveedores para prevenir los incidentes graves de seguridad.
- Ayudar a la protección de la información confidencial.
- Coordinar a los grupos que se ven impactados por la incidencia de manera centralizada. Indicadores de compromiso (STIX /TAXII, etc).
- Almacenar las evidencias que justifiquen todo el proceso de resolución de la incidencia.
- Promover una buena cultura de seguridad en todos los niveles de la Organización.

# Respuesta a incidentes... SOC:

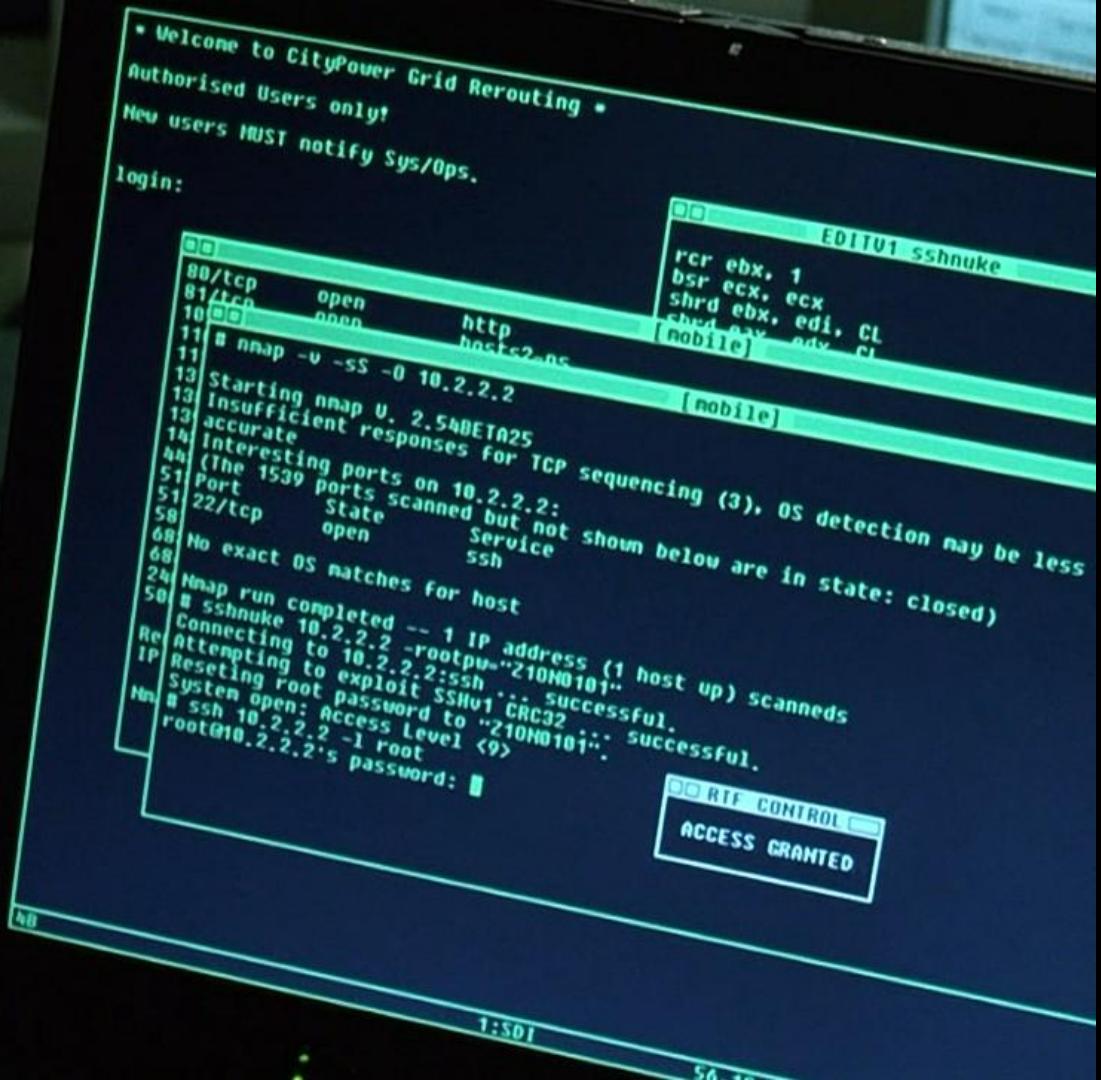
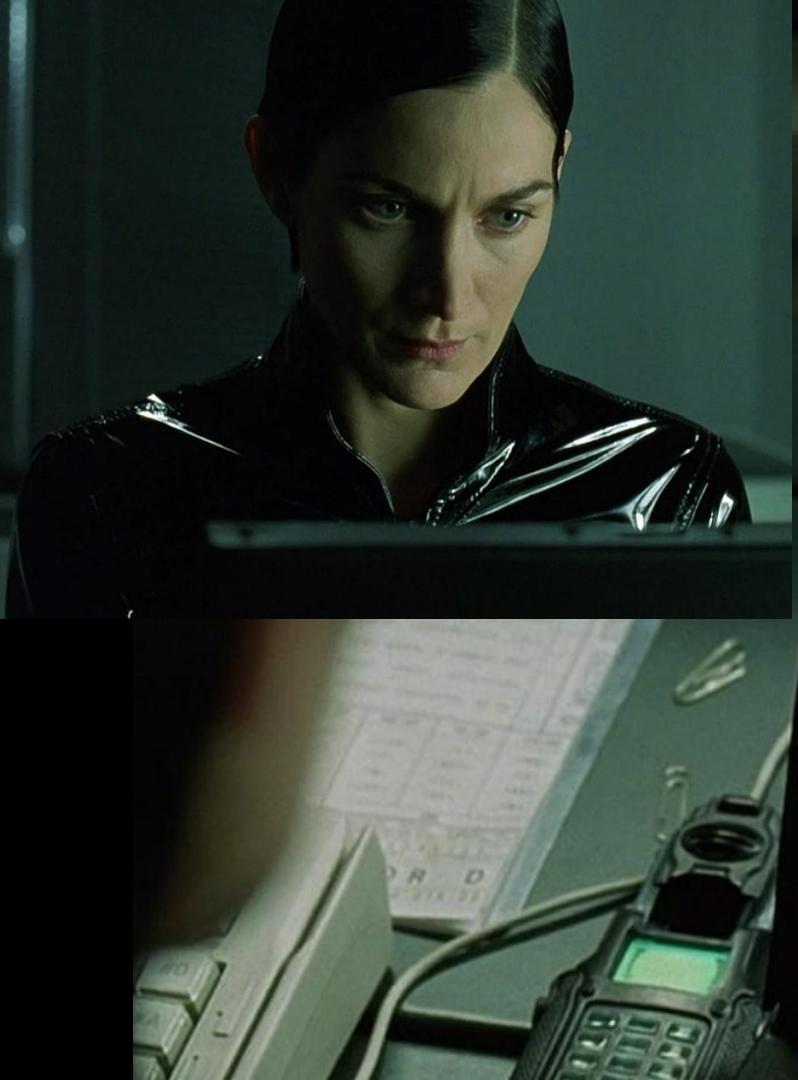


**SOC**: previene, monitoriza y da soporte. Ofrece servicios 24x7 de diagnóstico de vulnerabilidades, servicio de respuesta a incidentes, prevención de ataques, administración de riesgos y servicios de alerta antivirus. Los distintos servicios que ofrece a la organización son:

- Proporciona servicios de prevención que permite la identificación de alertas, vigilancia, análisis de vulnerabilidades y código malicioso.
- Proporciona servicios de operación en los que se van a analizar los logs para identificar situaciones peligrosas, monitorización de la seguridad perimetral y bastionado de arquitecturas.
- Proporciona servicios de mejora continua que ayudan a ejecutar planes de acción.
- Proporciona servicios de concienciación y divulgación para proporcionar cultura de seguridad a través de cursos, charlas y formación en general.

Nivel del Atacante	Motivación	Habilidades	Impacto
Bajo	<ul style="list-style-type: none"> <li>Script kiddies</li> <li>Autodidactas</li> </ul>	<ul style="list-style-type: none"> <li>▪ Sin conocimiento</li> <li>▪ Parecen inofensivos pero tienen éxito</li> <li>▪ Están socialmente aceptados</li> <li>▪ Robo rápido y fácil</li> </ul>	<ul style="list-style-type: none"> <li>▪ Impacto económico bajo</li> <li>▪ Fáciles de solventar</li> </ul>
Medio	<ul style="list-style-type: none"> <li>Autodidactas</li> <li>Activistas políticos</li> <li>Motivaciones económicas</li> </ul>	<ul style="list-style-type: none"> <li>▪ Conocimientos sobre seguridad</li> <li>▪ Entienden las vulnerabilidades</li> </ul>	<ul style="list-style-type: none"> <li>▪ Impacto económico medio-alto</li> <li>▪ Fácil de rastrear</li> </ul>
Alto	<ul style="list-style-type: none"> <li>Autodidactas</li> <li>Motivaciones económicas</li> <li>Activistas políticos</li> <li>Ataques contratados</li> </ul>	<ul style="list-style-type: none"> <li>▪ Conocimiento avanzado sobre seguridad</li> <li>▪ Pueden encontrar nuevas vulnerabilidades y escribir exploits</li> <li>▪ Pueden ocultar su trazabilidad</li> <li>▪ Seleccionan las víctimas de manera selectiva</li> </ul>	<ul style="list-style-type: none"> <li>▪ Alto impacto económico</li> <li>▪ Muy difícil o muy fácil de identificar <ul style="list-style-type: none"> <li>▪ Fácil: DoS</li> <li>▪ Difícil: Careto</li> </ul> </li> <li>▪ Difícil de rastrear</li> </ul>

ILUSTRACIÓN 3 PERFIL DE ATACANTES





## Read The Free Book

Want to get started with Kali Linux, but not sure how? Need to compile a custom kernel or build a custom Kali ISO? We've got a free Kali book for you! You can jump in right now and read the book either in online HTML, PDF or in printed form from Amazon.com.

## Take The Kali Training

Feeling adventurous? Interested in jumpstarting your infosec career? Looking to improve your command of Linux? Your journey starts here! Read along and test your skills with online training. Sign up for a free account to track your progress and get recognition.

[DOWNLOAD PDF](#)

[TAKE THE COURSE](#)

## Get Your KLCP Certification

Schedule your KLCP exam and get certified. Show off your newly gained skills and get recognition from potential employers. Learn about the Kali Linux Certified Professional certification, study the book and take the 80-question 90-minute exam with Pearson Vue.

[SCHEDULE EXAM](#)

### Become a Certified Penetration Tester Today

Enroll in the industry-leading certification program, designed by the creators of Kali Linux, and offered online exclusively through Offensive Security. [Learn More](#)

[Enroll Now](#)

CYBER ATTACK MANAGEMENT FOR METASPLOIT

# Armitage

DOWNLOAD

FAST AND EASY HACKING

MEDIA

MANUAL

FAQ

CONTACT

© 2010-2014 Strategic Cyber LLC

Connect: [Twitter](#) | [Facebook](#) | [LinkedIn](#) | [IRC](#) | [Blog](#) | [YouTube](#)



A 4834 personas les gusta esto. [Registrarse](#)  
para ver qué les gusta a tus amigos.



## Google Hacking Database

Filters

Reset All

Show  Quick Search 

Date Added	Dork	Category	Author
2018-12-20	inurl:admin.php inurl:admin ext:php	Pages Containing Login Portals	T3jv1l
2018-12-17	intitle: "Nexus Repository Manager"	Various Online Devices	Alfie
2018-12-14	inurl:LOG.txt X-System folder	Files Containing Juicy Info	B15mu7h
2018-12-14	inurl:webman/index.cgi	Pages Containing Login Portals	B15mu7h
2018-12-14	"Example: jane.citizen1"	Pages Containing Login Portals	B15mu7h
2018-12-14	intext:"EQ1PCI"	Pages Containing Login Portals	Kaligulah
2018-12-14	intext:password "Login Info" filetype:txt	Files Containing Juicy Info	Kevin Randall
2018-12-14	filetype:txt "Registration Code"	Files Containing Juicy Info	T3jv1l
2018-12-05	"login":	Pages Containing Login Portals	Gionathan Reale
2018-12-05	inurl:_cpanel/forgotpwd	Pages Containing Login Portals	B15mu7h
2018-12-04	"Powered by vShare"	Web Server Detection	CrimsonTorso
2018-12-04	inurl:/help/lang/en/help	Various Online Devices	TheCrypticSailor
2018-12-04	inurl:public.php inurl:service ext:php	Various Online Devices	Rootkit_Pentester
2018-12-04	filetype:xml config.xml passwordHash Jenkins	Files Containing Passwords	Kevin Randall
2018-12-04	intitle:ProFTPD Admin - V1.04	Various Online Devices	XLOMBOX

Showing 1 to 15 of 4,566 entries

FIRST PREVIOUS 2 3 4 5 ... 305 NEXT LAST

 Verified  Has App

Filters Reset All

Show  Search: 

Date	D	A	V	Title	Type	Platform	Author
2018-12-21				Netatalk < 3.1.12 - Authentication Bypass	Remote	Multiple	Jacob Baines
2018-12-21				SQLScan 1.0 - Denial of Service (PoC)	DoS	Windows	Rafael Pedrero
2018-12-21				Microsoft Windows - 'MsiAdvertiseProduct' Arbitrary File Read	Local	Windows	evil_polar_bear
2018-12-21				ZeusCart 4.0 - Cross-Site Request Forgery (Deactivate Customer Accounts)	WebApps	PHP	mqt
2018-12-21				Microsoft Edge 42.17134.1.0 - 'Tree::ANode::DocumentLayout' Denial of Service	DoS	Windows	Bogdan Kurinnoy
2018-12-21				AnyBurn 4.3 - Local Buffer Overflow (SEH)	Local	Windows	Matteo Malvica
2018-12-20				Erlang - Port Mapper Daemon Cookie RCE (Metasploit)	Remote	Multiple	Metasploit
2018-12-20				VBScript - MSXML Execution Policy Bypass	DoS	Windows	Google Security Research
2018-12-20				VBScript - VbsErase Reference Leak Use-After-Free	DoS	Windows	Google Security Research
2018-12-20				Base64 Decoder 1.1.2 - Local Buffer Overflow (SEH)	Local	Windows	bzyo
2018-12-20				XMPPlay 3.8.3 - '.m3u' Local Stack Overflow Code Execution	Local	Windows	s7acktrac3
2018-12-20				LanSpy 2.0.1.159 - Buffer Overflow (SEH) (Egghunter)	Local	Windows_x86	bzyo
2018-12-19				IBM Operational Decision Manager 8.x - XML External Entity Injection	WebApps	Multiple	Mohamed M.Fouad
2018-12-19				PDF Explorer 1.5.66.2 - Buffer Overflow (SEH)	Local	Windows	Achilles
2018-12-19				Yeswiki Cercopitheque - 'id' SQL Injection	WebApps	PHP	Mickael BROUTY

Showing 1 to 15 of 40,525 entries

FIRST PREVIOUS 2 3 4 5 ... 2702 NEXT LAST



about 



theme ▾

write down a command-line to see the help text that matches each argument

try `showthedocs` for explaining other languages

 EXPLAIN

## examples

- `:(){ :|:& };:`
- `for user in $(cut -f1 -d: /etc/passwd); do crontab -u $user -l 2>/dev/null; done`
- `file=$(echo `basename "$file"`)`
- `true && { echo success; } || { echo failed; }`
- `cut -d ' ' -f 1 /var/log/apache2/access_logs | uniq -c | sort -n`
- `tar zcf - some-dir | ssh some-server "cd /; tar xvzf -"`
- `tar xzvf archive.tar.gz`
- `find . -type f -print0`
- `ssh -i keyfile -f -N -L 1234:www.google.com:80 host`
- `git log --graph --abbrev-commit --pretty=oneline origin..mybranch`

# Respuesta a incidentes... Incident Response:

- NMAP <https://nmap.org/>
  - <https://hackertarget.com/nmap-online-port-scanner/>
- NESSUS / OpenVAS
  - <https://www.tenable.com/downloads/nessus>
  - <http://www.openvas.org/>
- Metasploit Framework <https://www.exploit-db.com/>
  - <https://www.metasploit.com/>
  - <http://fastandeasyhacking.com/>
- DVL-DVWA <http://www.dvwa.co.uk/>
  - <https://metasploit.help.rapid7.com/docs/metasploitable-2>
  - <https://github.com/rapid7/metasploitable3>
- Kali Linux (Backtrack) <https://www.kali.org/>
  - <https://www.parrotsec.org/>
  - <https://backbox.org/>
  - <https://www.blackarch.org/>
  - <https://labs.fedoraproject.org/en/security/>
  - <https://www.pentoo.ch/>



OWASP Zed Attack Proxy Project +

https://www.owasp.org/index.php/OWASP\_Zed\_Attack\_Proxy\_Project

Log in Request account

Page Discussion Read View source View history Search

# OWASP Zed Attack Proxy Project

Main Screenshots Talks News ZAP Gear Supporters Functionality Features Languages Roadmap Get Involved

## FLAGSHIP mature projects

Review this project.

The OWASP Zed Attack Proxy (ZAP) is one of the world's most popular free security tools and is actively maintained by hundreds of international volunteers\*. It can help you automatically find security vulnerabilities in your web applications while you are developing and testing your applications. Its also a great tool for experienced pentesters to use for manual security testing.

ZAP 2.7.0 is now available!

[Download ZAP](#)

Please help us to make ZAP even better for you by answering the [ZAP User Questionnaire](#)!

For a quick overview of ZAP and an introduction to the [official ZAP Jenkins plugin](#) see these tutorial videos on YouTube:



Quick Download

[Download OWASP ZAP!](#)

Donate to ZAP

[Donate](#)

News and Events

Please see the [News](#) and [Talks](#) tabs

Change Log

- [zaproxy](#)
- [zap-extensions](#)

Code Repo

- [zaproxy](#)
- [zap-extensions](#)

Email List

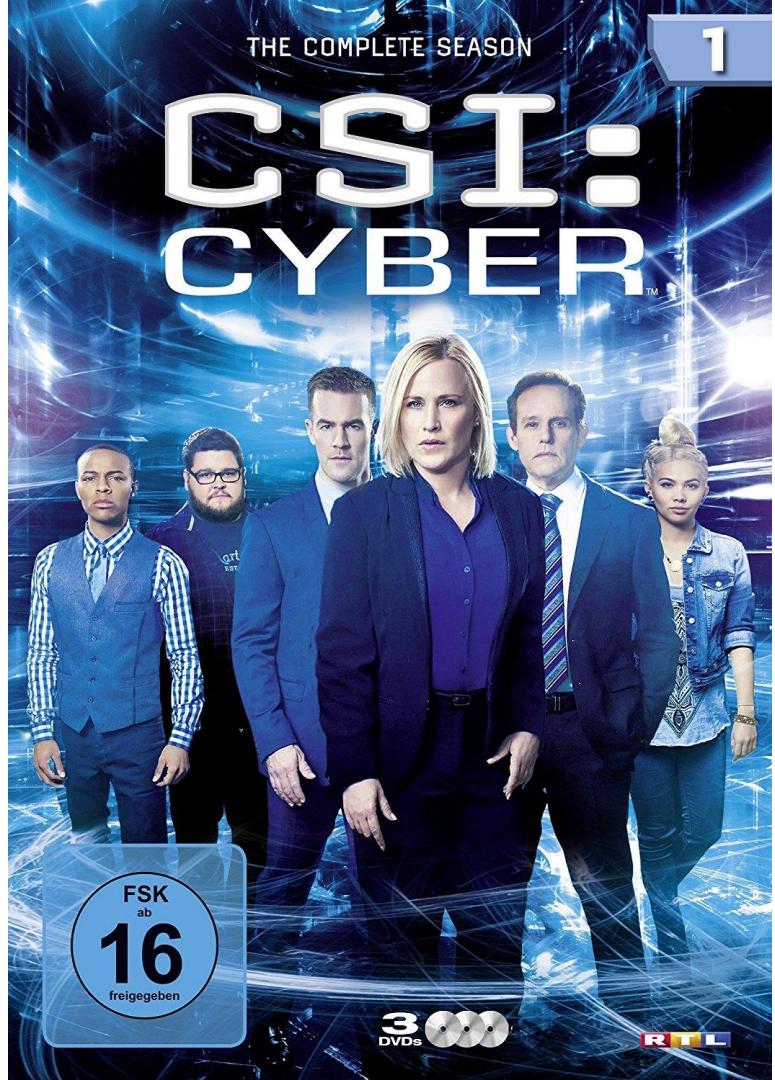
Questions? Please ask on the [ZAP User Group](#)

Project Leader

Project Leader  
Simon Bennetts @

Co-Project Leaders

Home About OWASP Acknowledgements Advertising AppSec Events Supporting Partners Books Brand Resources Chapters Donate to OWASP Downloads Funding Governance Initiatives Mailing Lists Membership Merchandise Presentations Press Projects Video Reference Activities Attacks Code Snippets Controls Glossary How To... Java Project .NET Project Principles Technologies Threat Agents Vulnerabilities Tools What links here Related changes Special pages Printable version Permanent link Page information





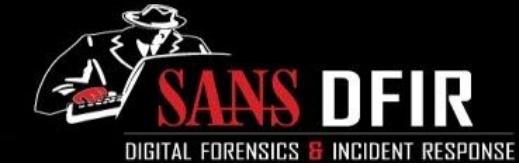
cases



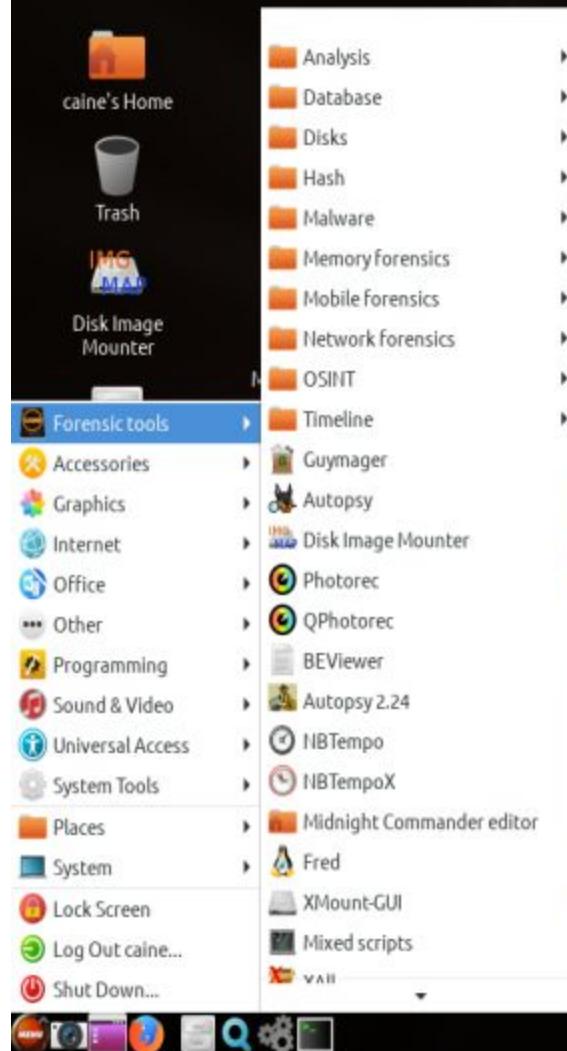
mount\_points

log2timeline-  
cheatsheet.pdfwindows-to-unix-  
cheatsheet.pdfMemory Forensics  
Cheat Sheet .pdfnetwork-forensics-  
cheatsheet.pdfBrochure\_  
SANSDFIR.pdfSIFT-Cheat-Sheet.  
pdfPoster\_Fall\_2013\_  
Evidence\_Of.pdfPoster\_2014\_Find\_  
Evil.pdf

```
x - sansforensics@siftworkstation: ~
sansforensics@siftworkstation:~$ 
```



DIGITAL FORENSICS &amp; INCIDENT RESPONSE



# Respuesta a incidentes... Incident Response:

## Análisis forense de un incidente de seguridad:

- Investigación u origen de un determinado incidente que requiere un análisis. Será necesario entender el contexto del problema.
- **Identificación** técnica de los sistemas involucrados en el proceso de análisis forense; Vector de entrada, propagación, etc.
- **Recolección.** Preservación de pruebas y evidencias, teniendo en cuenta que la información almacenada en los sistemas de origen no deberá de ser alterada ya que podría estar sujeta a alguna legislación o proceso jurídico.
- **Adquisición** de la información de los sistemas de origen intentando extraer información oculta.
- Análisis de la información obtenida de los sistemas de origen y **verificación** que logre dar explicación al incidente producido. **Preservación** y cadena de custodia de las evidencias.
- Informe de todo el proceso de análisis forense con las conclusiones obtenidas, indicando las posibles mejoras que se puedan implantar.

# CHAIN OF CUSTODY PRESERVATION

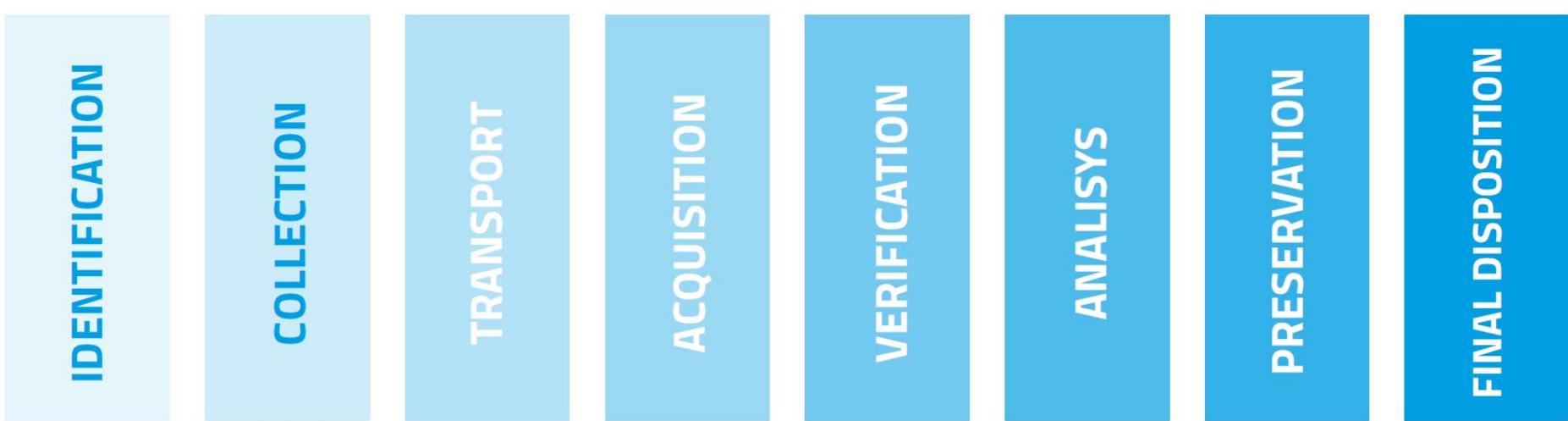


ILUSTRACIÓN 4 IMPORTANCIA DE LA CADENA DE CUSTODIA DE LA INFORMACIÓN

# Cyber-Sec... Nuevos Retos:

**Implicaciones y retos de las nuevas tecnologías:** Entorno cambiante, panorama complejo. Prima la movilidad y la conectividad.

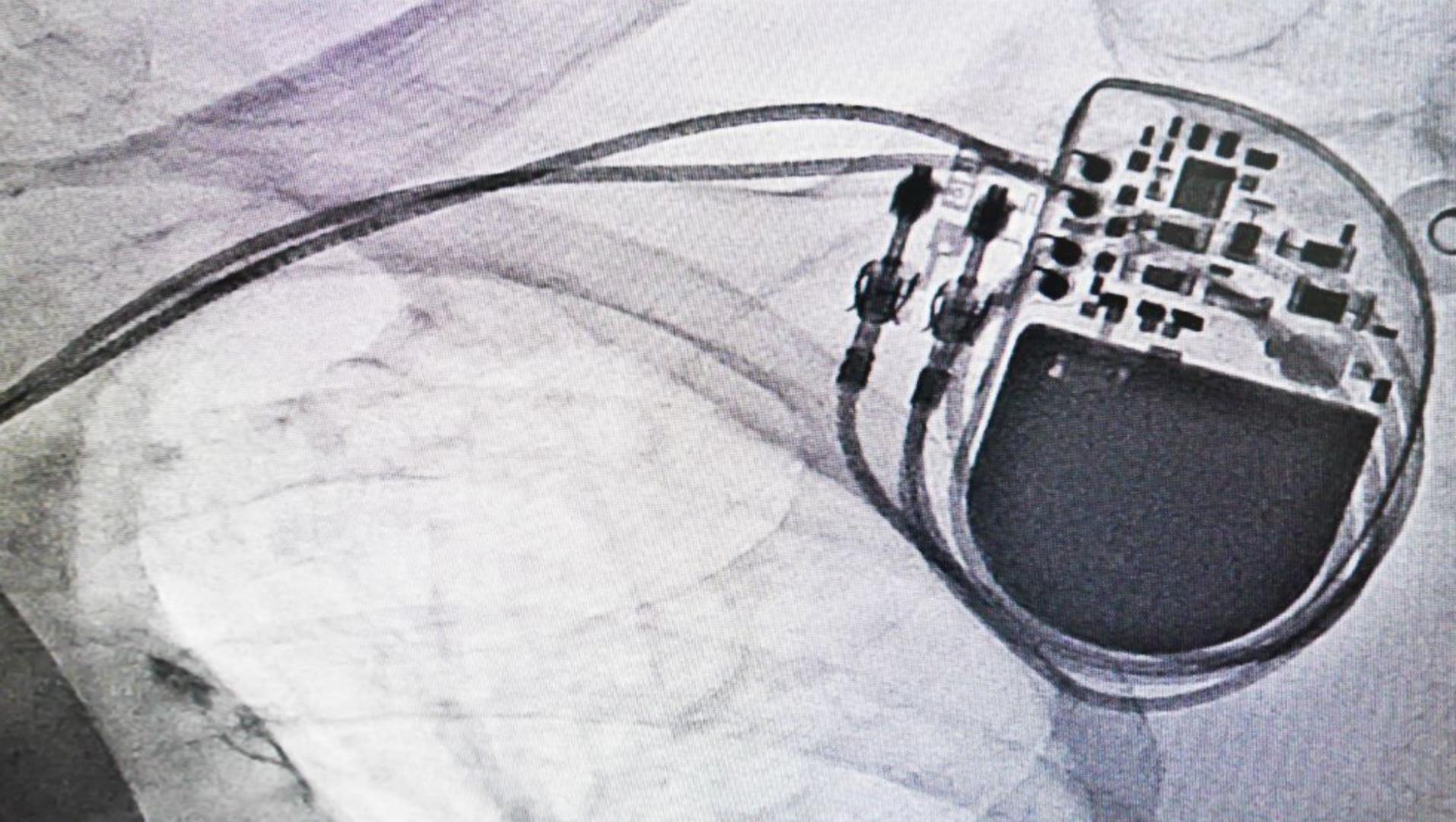
- Sistemas tecnológicos más avanzados.
- Amenazas más complejas.
- Ajuste del gasto presupuestario.
- Formación del personal.
- Alineamiento con el negocio.
- La seguridad como proceso transparente

The image shows a login form with two fields. The 'Username' field contains the value "' OR 1=1; /\*". The 'Password' field contains the value '\*/--'. Below the fields is a blue 'Log In' button.

Username  
' OR 1=1; /\*

Password  
\*/--

Log In





CYBERWAR



OD!SEA | VR

VR

VICELAND

GUÍA TV

CLUB

BLOG



CYBERWAR T1

LA SERIE

EPISODIOS

VÍDEOS



Ben Makuch se adentra en la geopolítica de la piratería informática y los sistemas de vigilancia, en un viaje por todo el mundo para reunirse con hackers, funcionarios gubernamentales y disidentes e investigar el ecosistema de la guerra cibernetica.

Compartelo en:





MICRO  
CANALES

14 CANALES TEMÁTICOS  
3 CONTENIDOS GRATIS POR CANAL

DESCARGA LA APP

OD!SEA | VR VR VICE LAND GUÍA TV CLUB BLOG



CYBERWAR T1

TEMPORADA 1 TEMPORADA 2

LA SERIE

EPISODIOS

VÍDEOS



CYBERWAR T2: EP.1. HACKING THE ELECTION

Episodio 1

Sabemos que Rusia hackeó el Comité Nacional del Partido Demócrata para influir en las elecciones de 2016. Pero trate de localizar a los hackers.

VER MÁS



CYBERWAR T2: EP.2. PUTIN TRUMPS AMERICA

Episodio 2

Los tropas de la OTAN se reúnen a lo largo de la frontera rusa, mientras las autoridades encacuchadas luchan con la intromisión electoral de Putin.

VER MÁS



CYBERWAR T2: EP.3. MEMETIC WARFARE

Episodio 3

Los memes con elarma nula fuerte de la derrota alternativa en la lucha cultural en línea de Estados Unidos, y utilizan el paisaje político e histórico.

VER MÁS



CYBERWAR T2: EP.4. CYBER KILL LISTS

Episodio 4

Estados Unidos constituye una máquina de matar global utilizando información para identificar y eliminar a sospechosos de terrorismo.

VER MÁS



CYBERWAR T2: EP.5. ACTIVIST LIVES MONITORED

Episodio 5

Las agencias de inteligencia se asocian con empresas para espionar a ciudadanos estadounidenses. Algunos activistas luchan contra esta cibervigilancia.

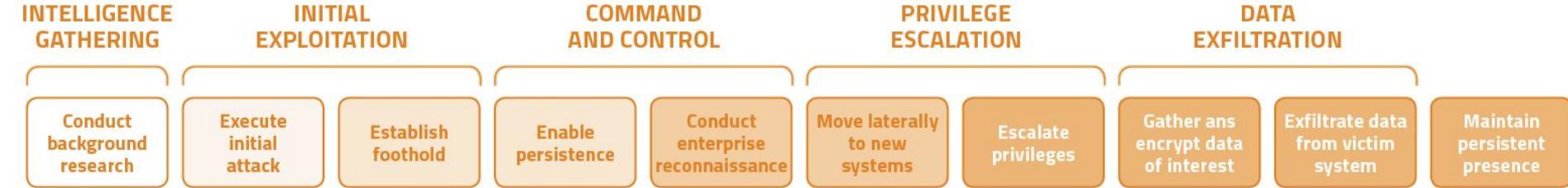
VER MÁS

VICE



# Cyber-Sec... Cyberwar:

- Ciberguerra, ciberterrorismo, hacktivismo, etc.
- Organizaciones criminales atacan gobiernos o empresas con fines económicos, políticos, reputacionales, etc.
  - APT
  - DDoS
  - Botnet
  - Ingeniería social
  - Virus y Troyanos
  - Ataques multivectoriales que combinen varios anteriores



# Cyber-Sec... APT:

Amenaza Avanzada Persistente:

- **Intelligence Gathering.** A lo largo de esta fase se busca toda la información posible sobre la víctima del ataque. Se utiliza la información existente en OSINT, ingeniería social y tantos medios como sean posibles para generar una estrategia de ataque.
- **Initial Exploitation.** Es el ataque inicial con el que se logra generar el acceso a nuestra víctima.
- **Command and Control.** En esta fase se establece la capacidad para convertir el ataque en persistente y se comienza la búsqueda interna dentro de la organización.
- **Privilege Escalation.** En esta fase, se busca moverse a un usuario con mayores privilegios que nos da la capacidad de llegar hasta la información objetivo del ataque.
- **Data Exfiltration.** Es la fase en la que se obtiene la información objetivo y se explota de manera que sea beneficiosa para el atacante. Una vez aprovechada la información, no se abandona el acceso, por lo que se sigue teniendo capacidad de actuación.

# Cyber-Sec... APT:

- En el año 2003 tuvo lugar “Titan Rain”, un ataque que realizó intrusiones en las redes de Departamento de Defensa de los EEUU, la NASA y varias empresas de defensa. Dio origen al concepto “Advanced Persistent Threat (APT)” ya que se ha considerado como un ataque lanzado por un grupo organizado, sofisticado y coordinado contra una máquina o red objetivo durante un periodo prolongado con propósitos de espionaje y no de alguna ventaja económica.
- En el año 2008 tuvo lugar el conocido ataque denominado “Buckshot Yankee” tipo APT, diseñado para usar memorias USB como el vector de ataque que dio lugar su prohibición en las redes del Departamento de Defensa. Tuvo un impacto operacional grande pues consiguió entrar en sistemas clasificados y no se sabe cuanta información consiguió extraer el malware. El departamento de defensa de Estados Unidos tardó 14 meses en quitar el gusano de su red y el incidente fue impulsor para la creación de USCYBERCOM mando de Ciberdefensa con la misión de llevar a cabo la planificación, coordinación, dirección y conducción de las operaciones militares en el ciberespacio.

## INVESTIGACIÓN

# El gran robo de banco: el APT Carbanak

GReAT - Febrero 16, 2015. 7:20 pm

[Download Full Report PDF \(eng\)](#)

La historia de Carbanak comenzó cuando un banco de Ucrania nos pidió ayuda con una investigación forense: Le estaban robando misteriosamente el dinero desde los cajeros automáticos. Al principio creímos que se trataba del programa malicioso **Tyupkin**. Sin embargo, después de investigar el disco duro del sistema de cajeros automáticos, no logramos encontrar nada, salvo una inusual configuración VPN (la máscara de red estaba fijada en 172.0.0.0).

En ese momento, nos pareció como un ataque más de programas maliciosos. Ni nos imaginábamos en ese entonces que pocos meses después uno de nuestros colegas recibiría una llamada a las tres de la madrugada. Era un gerente de cuenta que nos pedía que hicieramos algunas llamadas urgentes. Al otro lado de la línea se encontraba el jefe de estrategia de un banco ruso. Uno de sus sistemas alertaba sobre envíos de datos desde su controlador de dominio hasta China.

Cuando llegamos a sus oficinas, logramos rápidamente encontrar el programa malicioso en el sistema. Escribimos un script batch para eliminar el programa de un PC infectado, y lo ejecutamos en todos los ordenadores del banco. Lo hicimos varias veces hasta estar seguros de que todos los equipos estaban limpios. Por supuesto, guardamos muestras que nos permitieron descubrir el programa malicioso Carbanak.

## Cómo funciona

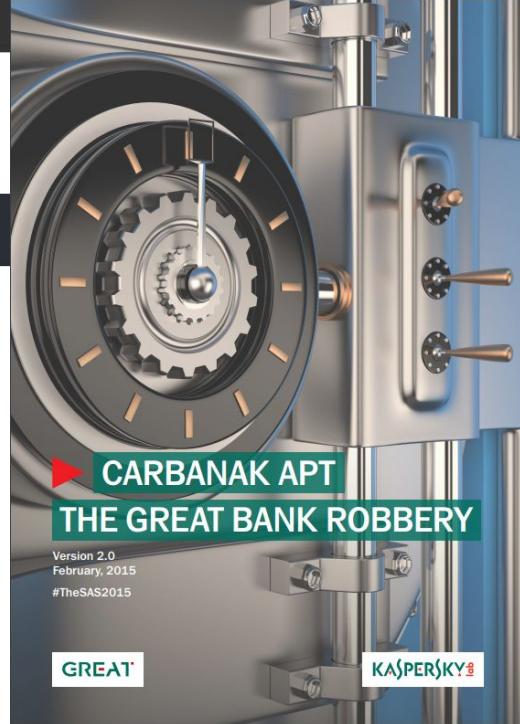
Un análisis forense más exhaustivo nos condujo al punto inicial de la infección: un mensaje de correo tipo spear-phishing con un adjunto CPL. En otros casos se utilizaron documentos Word que explotaban vulnerabilidades conocidas. Después de ejecutar el shellcode se instala en el sistema una puerta trasera basada en Carbero. Esta puerta trasera es lo que hoy



## Kaspersky Lab

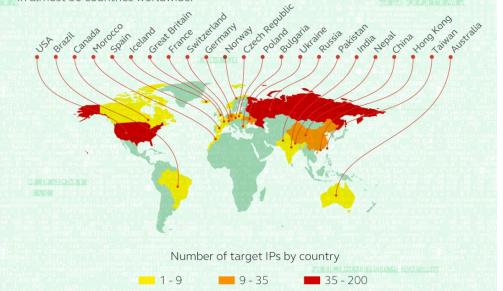
Ha recibido el premio Gartner Peer Insights Customers' Choice de 2018 en la categoría de Plataformas de Protección Endpoint

[Descubrir más](#)



## Map of Carbanak targets

Up to 100 financial institutions were hit at more than 300 IP addresses in almost 30 countries worldwide.



# Cyber-Sec... APT:

- Otro famoso ejemplo de APT es “Stuxnet”, ataque sufrido por Irán, siendo uno de los ataques cibernéticos más grandes de la historia. Los sistemas de control SCADA de la central nuclear de Bushehr, así como de otras industrias, se vieron afectados por un virus de una potencia sin precedentes, consiguiendo retrasar la producción de uranio enriquecido. Se trata de una APT que se compone de un gusano que se propaga a través de unidades USB, un exploit de Windows, un rootkit para evitar su descubrimiento y un troyano que busca específicamente un modelo particular de los sistemas SCADA.
- APT Carbanak [https://krebsonsecurity.com/wp-content/uploads/2015/02/Carbanak\\_APT\\_eng.pdf](https://krebsonsecurity.com/wp-content/uploads/2015/02/Carbanak_APT_eng.pdf)  
<https://securelist.lat/el-gran-robo-de-banco-el-apt-carbanak/67508/>

# Fancy Bear

From Wikipedia, the free encyclopedia

**Fancy Bear** (also known as **APT28**, **Pawn Storm**, **Sofacy Group**, **Sednit** and **STRONTIUM**)<sup>[2]</sup> is a cyber espionage group. Cybersecurity firm CrowdStrike has said with a medium level of confidence that it is associated with the Russian military intelligence agency GRU.<sup>[4][5]</sup> The Foreign and Commonwealth Office,<sup>[6]</sup> and security firms SecureWorks,<sup>[7]</sup> ThreatConnect,<sup>[8]</sup> and Fireeye's Mandiant,<sup>[9]</sup> have also said the group is sponsored by the Russian government. In 2018, an indictment by the United States Special Counsel identified Fancy Bear as two GRU units known as **Unit 26165** and **Unit 74455**.<sup>[3][2]</sup>

The name "Fancy Bear" comes from a coding system security researcher Dmitri Alperovitch uses to identify hackers.<sup>[10]</sup>

Likely operating since the mid-2000s, Fancy Bear's methods are consistent with the capabilities of state actors. The group targets government, military, and security organizations, especially Transcaucasian and NATO-aligned states. Fancy Bear is thought to be responsible for cyber attacks on the German parliament, the French television station TV5Monde, the White House, NATO, the Democratic National Committee, Organization for Security and Co-operation in Europe and the campaign of French presidential candidate Emmanuel Macron.<sup>[11]</sup>

The group promotes the political interests of the Russian government, and is known for hacking Democratic National Committee emails to help Donald Trump during the United States 2016 presidential elections.<sup>[12]</sup>

Fancy Bear is classified by Fireeye as an advanced persistent threat.<sup>[9]</sup> Among other things, it uses zero-day exploits, spear phishing and malware to compromise targets.

Contents [hide]

## Fancy Bear

	Модный мишка
<b>Formation</b>	c. 2004–2007 <sup>[2]</sup>
<b>Type</b>	Advanced persistent threat
<b>Purpose</b>	Cyberespionage, cyberwarfare
<b>Region</b>	Russia
<b>Methods</b>	Zero-days, spearphishing, malware
<b>Official language</b>	Russian
<b>Parent organization</b>	GRU <sup>[1][2][3]</sup>
<b>Affiliations</b>	Cozy Bear
<b>Formerly called</b>	APT28 Pawn Storm Sofacy Group Sednit STRONTIUM Tsar Team Threat Group-4127 Grizzly Steppe (when combined with Cozy Bear)

# Lazarus Group

From Wikipedia, the free encyclopedia

**Lazarus Group** (also known as **HIDDEN COBRA**)<sup>[1]</sup> is a **cybercrime** group made up of an unknown number of individuals.

While not much is known about the Lazarus Group, researchers have attributed many cyber attacks to them over the last decade.

## Contents [hide]

- 1 History
  - 1.1 Operation Blockbuster
  - 1.2 Operation Flame
  - 1.3 Ten Days of Rain
  - 1.4 Sony breach
  - 1.5 Cryptocurrency attacks
- 2 References
  - 2.1 Sources

## History [edit]

The earliest known attack that the group is responsible for is known as "Operation Troy", which took place from 2009–2012.

This was a cyber-espionage campaign that utilized unsophisticated **distributed denial-of-service attack** (DDoS) techniques to target the South Korean government in Seoul. They are also responsible for attacks in 2011 and 2013. It is possible that they were also behind a 2007 attack targeting South Korea, but that is still uncertain.<sup>[2]</sup> A notable attack that the group is known for is the **2014 attack on Sony Pictures**. The Sony attack used more sophisticated techniques and highlighted how advanced the group has become over time.

**WANTED BY THE FBI**  
**PARK JIN HYOK**  
Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud (Computer Intrusion)

**DESCRIPTION**

Aliases: Pak Jin Hee, Jin Hyok Park  
Place of Birth: Democratic People's Republic of Korea (North Korea)  
Hair: Black  
Eyes: Brown  
Race: Asian  
Languages: English, Korean

**REMARKS**

Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Export" or the Korean Export Joint Venture in addition to activities conducted on behalf of North Korea's Ministry of National Defense General Bureau.

**CAUTION**

Park is alleged to be a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the most significant cyberattacks in recent years, including the WannaCry ransomware attack, the NotPetya ransomware attack, and the Mirai botnet attack across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computers across the globe.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles

**FBI wanted notice for one of the hackers of Lazarus Group, Pak Jin-hyok [es]**



## TE-SAT 2018

New EU Terrorism Situation and Trend Report describes terrorist incidents and activities on European soil.

[LEARN MORE](#)

Latest

## UPDATES



French Gendarmerie capture key members of Armenian mafia

[PRESS RELEASE](#)

13 car thieves with expensive taste arrested by the French Gendarmerie

[PRESS RELEASE](#)

First report of the observatory function on encryption

[PUBLICATIONS](#)

Are you looking for a new career challenge?

Apply now at Europol

[VACANCIES](#)

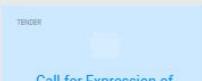
Criminal gang recruiting Portuguese women into sham marriages dismantled

[PRESS RELEASE](#)

Fraud on the tennis court: criminal network gained millions fixing professional matches

[PRESS RELEASE](#)

Swoop against German-Lithuanian organised crime gang

[PRESS RELEASE](#)

Call for Expression of Interest: Training and Expert Services for Cybercrime Examinations and Investigations

[PROCUREMENT](#)

# ORACLE CLOUD

Engineered For Heroes

[www.oracle.com/Ironman3](http://www.oracle.com/Ironman3)



TM & © 2013 MARVEL. www.marvel.com

MARVEL

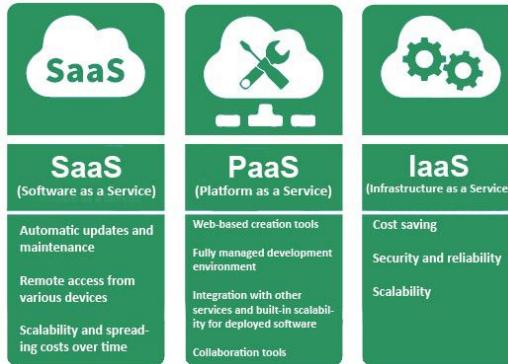
MARVEL  
**IRON MAN 3**

**ORACLE®**

# Cyber-Sec... CLOUD:

Nuevo modelo de arquitectura. Objetivo: facilitar recursos (almacenado, proceso, servicios, etc.) favoreciendo la disponibilidad (instantánea descentralizada), flexibilidad y escalabilidad.

- Privacidad de la información
- Control de acceso
- Tratamiento de nuevos tipos de vulnerabilidades
- Requisitos legales



# Cyber-Sec... BYOD:

## Ventajas:

- Los trabajadores trabajan con mayor productividad al disponer de las comodidades de su dispositivo, según sus configuraciones personales favoreciendo así a una mayor calidad en la colaboración con los compañeros y un rendimiento mayor.
- Mayor satisfacción en el trabajo al poder disponer durante su día a día de los mismos dispositivos que utilizan durante su vida cotidiana, favoreciendo a la satisfacción de los empleados.
- Este tipo de políticas va a favorecer en el ahorre de los costes de mantenimiento y compra de dispositivos, para que los empleados dispongan de los mismos (tablet, portátiles, smartphones, móviles, etc.).
- Establecer este tipo de políticas ayuda al empleado trabajar con mayor flexibilidad, disponiendo de las herramientas de trabajo durante su vida cotidiana, aportando mayor flexibilidad para elegir el momento y el lugar para desarrollar sus tareas, incluso fuera de horario laboral.

# Cyber-Sec... BYOD:

## Inconvenientes:

- La protección de la información supone un reto para las empresas que asumen este tipo de políticas ya que algunos dispositivos que pueden acceder a tu red no cuenten con las medidas de protección adecuadas y consumen información confidencial que se descarguen de manera local en el dispositivo. Si la organización no cuenta con cierto control para prevenir este tipo de situaciones puede ser un riesgo para la Organización.
- En el caso de que un dispositivo infectado se conecte a la red, esto puede suponer que algún dispositivo resulte infectado con algún tipo de aplicación perjudicial.
- Asumiendo este tipo de políticas, la cantidad de dispositivos que pueden consumir procesamiento en la red de un Organización aumenta de manera considerable por lo que se hace necesario que el sistema sea escalable para poder soportar la conexión de estos dispositivos sin que se vea perjudicada la capacidad o la disponibilidad de la red.
- Se hace necesario que existan departamentos que den soporte y mantenimiento a la problemática que supone el acceso de estos dispositivos a la red y será necesario la monitorización de los mismos con la intención de velar por la seguridad de los sistemas.

# Cyber-Sec... BYOD:

Mobile Device Management (**MDM**):

- Instalación y actualización de aplicaciones.
- Control de aplicaciones.
- Seguimiento y monitorización. Geolocalización.
- Bloqueo de las actividades.
- Borrado remoto de información.



• python

Please update from master branch or check for new releases.

System check identified no issues (0 silenced).

April 02, 2018 - 10:31:08

Django version 1.11.3, using settings 'MobSF.settings'

Starting development server at http://127.0.0.1:8000/

Quit the server with CONTROL-C.

[02/Apr/2018 10:33:34] "GET / HTTP/1.1" 200 7692

[02/Apr/2018 10:33:35] "GET /static/css/bootstrap.min.css HTTP/1.1"

[02/Apr/2018 10:33:35] "GET /static/js/jquery.min.js HTTP/1.1" 200 9

[02/Apr/2018 10:33:35] "GET /static/css/dropzone.css HTTP/1.1" 200 1

[02/Apr/2018 10:33:35] "GET /static/css/cover.css HTTP/1.1" 200 2850

[02/Apr/2018 10:33:35] "GET /static/js/ie-emulation-modes-warning.js

00 2132

[02/Apr/2018 10:33:35] "GET /static/js/dropzone.js HTTP/1.1" 200 644

[02/Apr/2018 10:33:35] "GET /static/js/bootstrap.min.js HTTP/1.1" 200

[02/Apr/2018 10:33:35] "GET /static/js/viewport-bug-workaround.

200 694

[02/Apr/2018 10:33:35] "GET /static/img/MobSF\_Logo\_small.png HTTP/1.

[02/Apr/2018 10:33:35] "GET /static/favicon.ico HTTP/1.1" 200 370070

[02/Apr/2018 10:33:35] "GET /static/fonts/glyphicons-halflings-regul

1.1" 200 25320

]



Emulator



SocialDrive\_v4.2.5  
apkpure.com.apk



LinkedIn\_v4.1.156  
apkpure.com.apk



CyRSocial  
Conductores y Red  
Social\_v1.1.17\_ap...



Lookout Security  
Antivirus\_v10.21.1-  
71c0cca\_apkpure...

• Mobile Security Framework - Mozilla Firefox

1. Documentation · MobsF · Mobile Security Framework

127.0.0.1:8000 | C | Q mobsf

MOBSF

Drag files here or click Upload & Analyze

Upload & Analyze

Search MD5

Recent Scans | About

© 2018 Mobile Security Framework - MobSF v0.9.5.2 Beta. All Rights Reserved

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... x

Icons: File, Folder, Home, Stop, Refresh, Back, Forward, Search, Help, Address Bar, Tab, Window Control Buttons, Footer Links.

# Cyber-Sec... Virtualización:

- Un servidor físico puede alojar varios servidores virtualizados.
- Hypervisor: Virtual Machine Monitor (VMM).

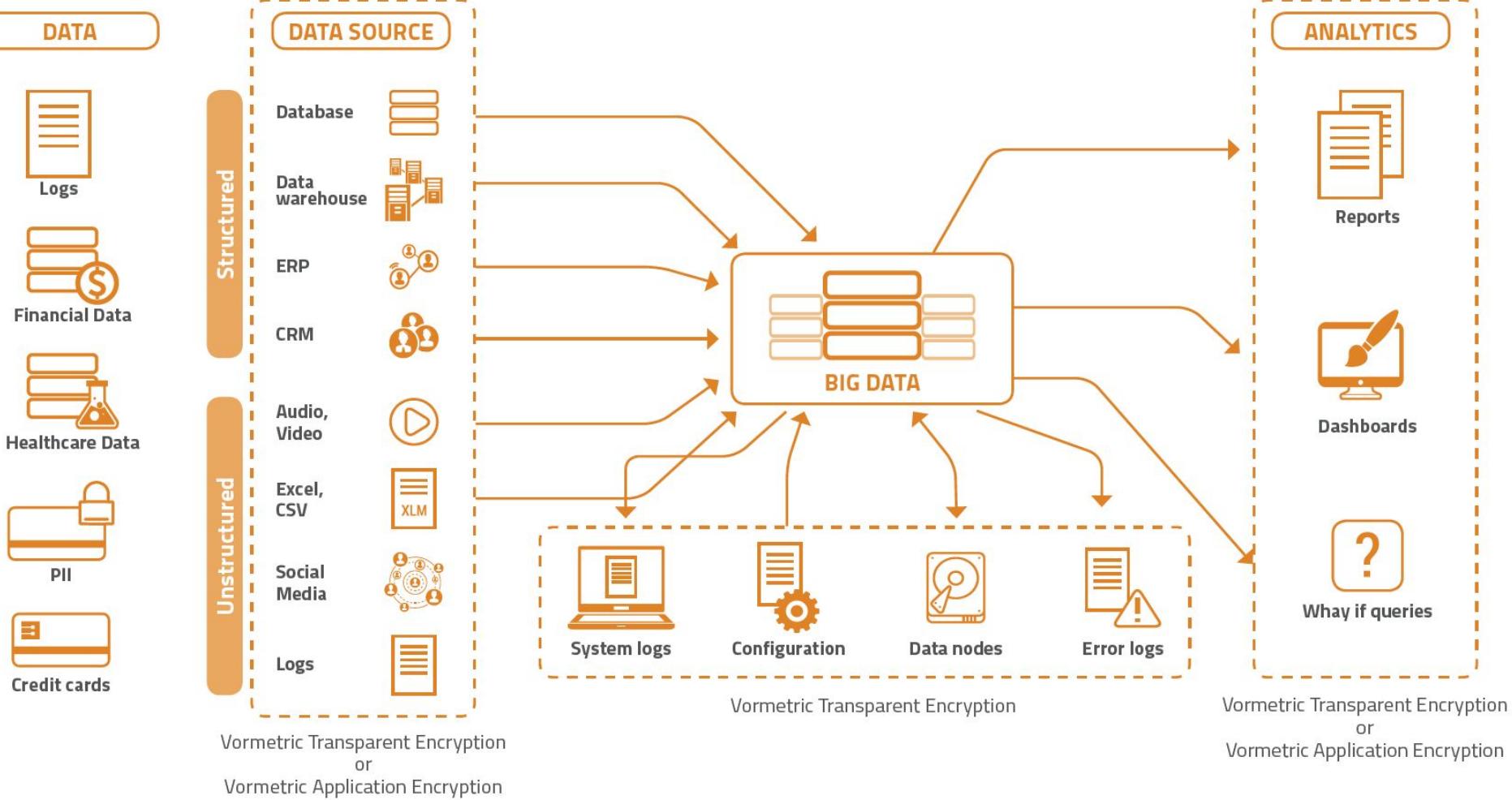
Tipos de virtualizaciones:

- Virtualización de red.
- Virtualización de aplicaciones.
- Virtualización de escritorio. Ej. Citrix

# Cyber-Sec... Virtualización:

## Beneficios:

- Disminuye el número de dispositivos físicos lo que deriva en menor espacio para su almacenaje y ahorro de costes ante la compra y mantenimiento del hardware.
- Aislar los riesgos operativos a la hora de realizar cambios en producción, al no impactar en el resto de máquinas.
- Mayor escalabilidad a la hora de ampliar la capacidad y rendimiento de los equipos de los que dispone el CPD.
- Desplegar distintos sistemas, con su correspondiente configuración, sobre una misma plataformas hardware.



# Cyber-Sec... Big Data:

Tipo de datos que a va poder explotar este tipo de tecnología es ilimitado:

- Contenido web y de redes sociales.
- Máquina a máquina; analizar y medir determinados eventos.
- Datos de transacciones: registro de llamadas, etc.
- Biométricos.
- Información propia de los usuarios: mensajes, correos, llamadas, etc.