



Bloque 1.- Introducción.

Introducción



Ciberseguridad – Máster Computación e IoT
Juan Carlos Gámez Granados



Tabla de contenidos

- **Conceptos**
- **Seguridad de la Información**
- **IoT: Internet of Things**

Tabla de contenidos

- **Conceptos**
- Seguridad de la Información
- IoT: Internet of Things

Conceptos

- **Activos**
 - Un activo es cualquier cosa de **valor** para la organización. Incluye personas, equipos, recursos y datos.
- **Amenaza**
 - Una amenaza es un **peligro** potencial para los activos, los datos o la funcionalidad de la red de una empresa. Tipos:
 - Robo de información
 - Pérdida y manipulación de datos
 - Robo de identidad
 - Interrupción de servicio

Conceptos

- Amenazas

ENISA Threat Landscape 15 Top Threats in 2020



EUROPEAN UNION AGENCY
FOR CYBERSECURITY 



www.enisa.europa.eu

For more information: <https://www.enisa.europa.eu/topics/etl>



Conceptos

- Amenazas

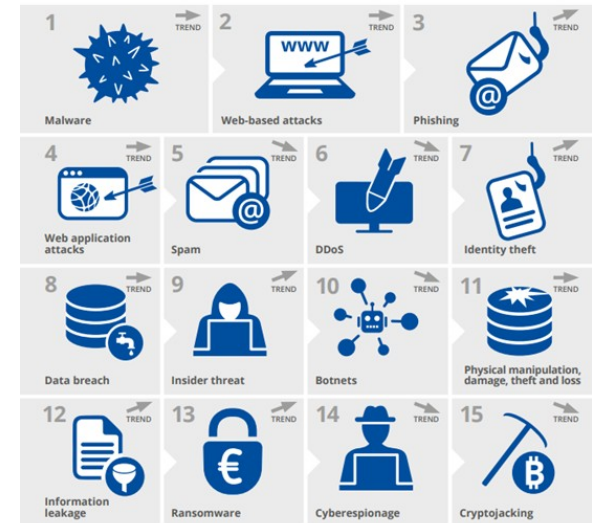
- ENISA Threat Landscape 2021

(<https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021>)

1. Ransomware
2. Malware
3. Cryptojacking
4. E-mail related threats
5. Threats against data
6. Threats against availability and integrity
7. Disinformation – misinformation
8. Non-malicious threats
9. Supply-chain attacks

15 Top Threats in 2020

EUROPEAN UNION AGENCY
FOR CYBERSECURITY



(<https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks>)

Conceptos

- **Vulnerabilidad**

- Una vulnerabilidad es una **debilidad** en un sistema, o su diseño, que podría ser explotada por una amenaza. Tipos:
 - Tecnológicas (protocolo -TCP/IP, S.O., equipo, ...)
 - De configuración (cuentas no seguras, contraseñas fáciles, configuraciones predeterminadas, no seguras, malas, ...)
 - De política de seguridad (falta de política de seguridad, no aplicación de política de seguridad o aplicación no continuada, plan de recuperación, ...)
- CVE (Common Vulnerabilities and Exposures), Mitre (<https://cve.mitre.org/>)
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-9527>)

- **Exploit**

- Un exploit es un **mecanismo** para tomar ventaja de una vulnerabilidad. (MITRE ATT&CK - <https://attack.mitre.org/>)

Conceptos

- Vulnerabilidad
 - CVE

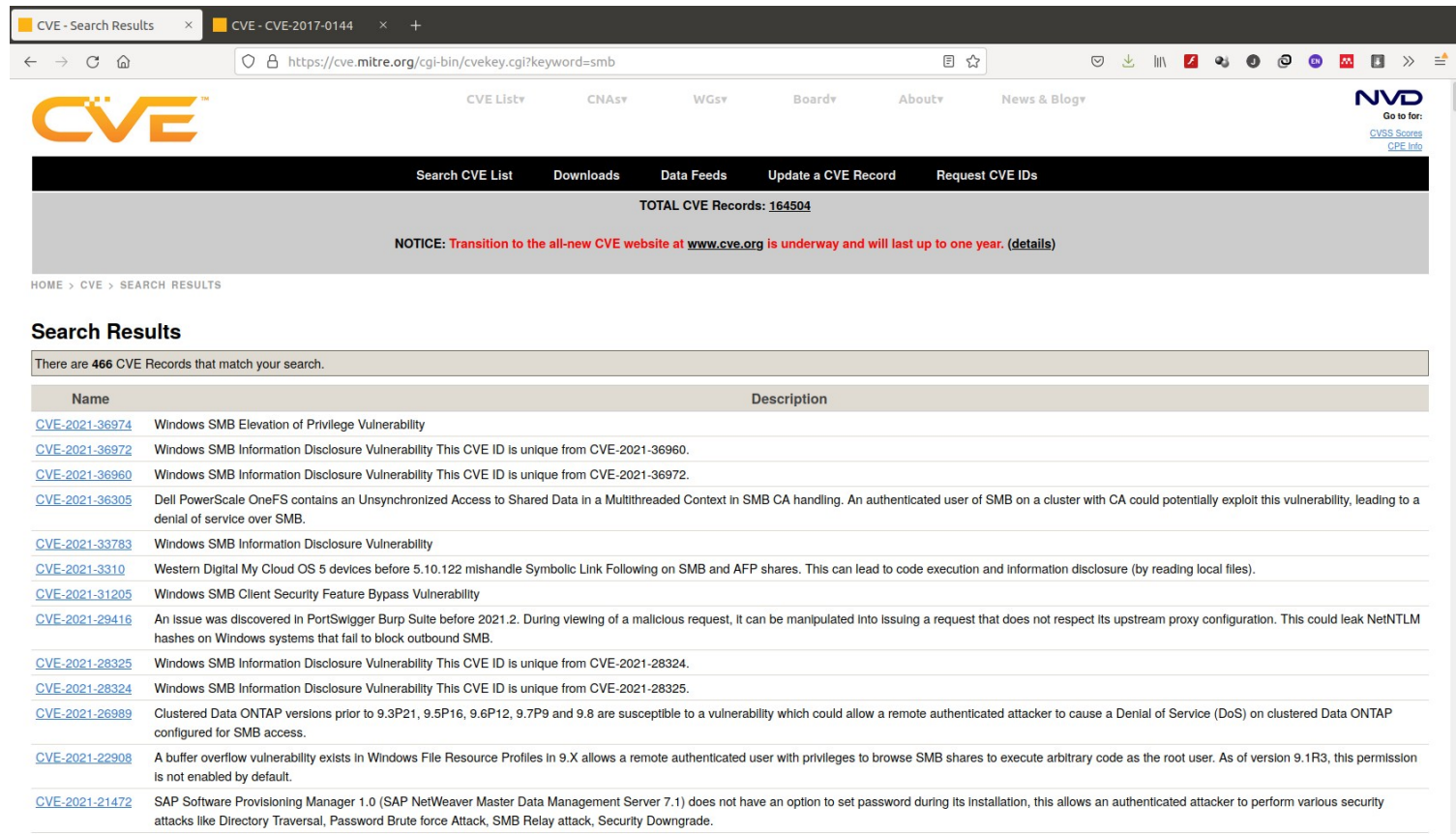
The screenshot shows the CVE website interface. At the top, there's a navigation bar with links for CVE List, CNAs, WGs, Board, About, and News & Blog. Below this is a search bar and a list of links: Search CVE List, Downloads, Data Feeds, Update a CVE Record, and Request CVE IDs. A prominent notice states: "NOTICE: Transition to the all-new CVE website at www.cve.org is underway and will last up to one year. (details)". The main content area is divided into several sections: CVE News, CVE Podcast, CVE Blog, Become a CNA, and Newest CVE Records. The Become a CNA section includes a world map and a list of benefits. The Newest CVE Records section shows a tweet about a CVE-2021-42338 vulnerability.

Page Last Updated or Reviewed: October 12, 2021
https://cve.mitre.org/cve/cna.html#become_a_cna



Conceptos

- Vulnerabilidad
 - CVE – search CVE List - smb



The screenshot shows the CVE Mitre search results page for the keyword 'smb'. The page displays a total of 466 CVE records. A notice indicates a transition to the new CVE website at www.cve.org is underway and will last up to one year. The search results are listed in a table with columns for Name and Description.

Name	Description
CVE-2021-36974	Windows SMB Elevation of Privilege Vulnerability
CVE-2021-36972	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-36960.
CVE-2021-36960	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-36972.
CVE-2021-36305	Dell PowerScale OneFS contains an Unsynchronized Access to Shared Data in a Multithreaded Context in SMB CA handling. An authenticated user of SMB on a cluster with CA could potentially exploit this vulnerability, leading to a denial of service over SMB.
CVE-2021-33783	Windows SMB Information Disclosure Vulnerability
CVE-2021-33110	Western Digital My Cloud OS 5 devices before 5.10.122 mishandle Symbolic Link Following on SMB and AFP shares. This can lead to code execution and information disclosure (by reading local files).
CVE-2021-31205	Windows SMB Client Security Feature Bypass Vulnerability
CVE-2021-29416	An issue was discovered in PortSwigger Burp Suite before 2021.2. During viewing of a malicious request, it can be manipulated into Issuing a request that does not respect its upstream proxy configuration. This could leak NetNTLM hashes on Windows systems that fail to block outbound SMB.
CVE-2021-28325	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28324.
CVE-2021-28324	Windows SMB Information Disclosure Vulnerability This CVE ID is unique from CVE-2021-28325.
CVE-2021-26989	Clustered Data ONTAP versions prior to 9.3P21, 9.5P16, 9.6P12, 9.7P9 and 9.8 are susceptible to a vulnerability which could allow a remote authenticated attacker to cause a Denial of Service (DoS) on clustered Data ONTAP configured for SMB access.
CVE-2021-22908	A buffer overflow vulnerability exists in Windows File Resource Profiles in 9.X allows a remote authenticated user with privileges to browse SMB shares to execute arbitrary code as the root user. As of version 9.1R3, this permission is not enabled by default.
CVE-2021-21472	SAP Software Provisioning Manager 1.0 (SAP NetWeaver Master Data Management Server 7.1) does not have an option to set password during its installation, this allows an authenticated attacker to perform various security attacks like Directory Traversal, Password Brute force Attack, SMB Relay attack, Security Downgrade.



Conceptos

- Vulnerabilidad

- CVE – search CVE List – smb - CVE-2017-0144

The screenshot shows the CVE Mitre website interface. At the top, there's a navigation bar with links like 'CVE List', 'CNA's', 'WG's', 'Board', 'About', and 'News & Blog'. Below this, a search bar and navigation links are visible. The main content area displays the CVE-2017-0144 details. It includes a 'Description' section with text about the SMBv1 server vulnerability in Microsoft Windows. Below the description is a 'References' section with a list of links to related resources, including BID, URL, CONFIRM, and EXPLOIT-DB entries. The page also features a 'Printer-Friendly View' link and a 'Go to for: CVSS Scores CPE info' link.

CVE - CVE-2017-0144

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144

CVE

CVE List CNA's WG's Board About News & Blog

NVD

Go to for: CVSS Scores CPE info

Search CVE List Downloads Data Feeds Update a CVE Record Request CVE IDs

TOTAL CVE Records: 164504

NOTICE: Transition to the all-new CVE website at www.cve.org is underway and will last up to one year. (details)

HOME > CVE > CVE-2017-0144

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.

- BID:96704
- URL:<http://www.securityfocus.com/bid/96704>
- CONFIRM:<https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf>
- CONFIRM:<https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf>
- CONFIRM:<https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144>
- EXPLOIT-DB:41891
- URL:<https://www.exploit-db.com/exploits/41891/>
- EXPLOIT-DB:41987
- URL:<https://www.exploit-db.com/exploits/41987/>
- EXPLOIT-DB:42030
- URL:<https://www.exploit-db.com/exploits/42030/>



Conceptos

- Vulnerabilidad

- CVE – search CVE List – mqtt - CVE-2019-5432

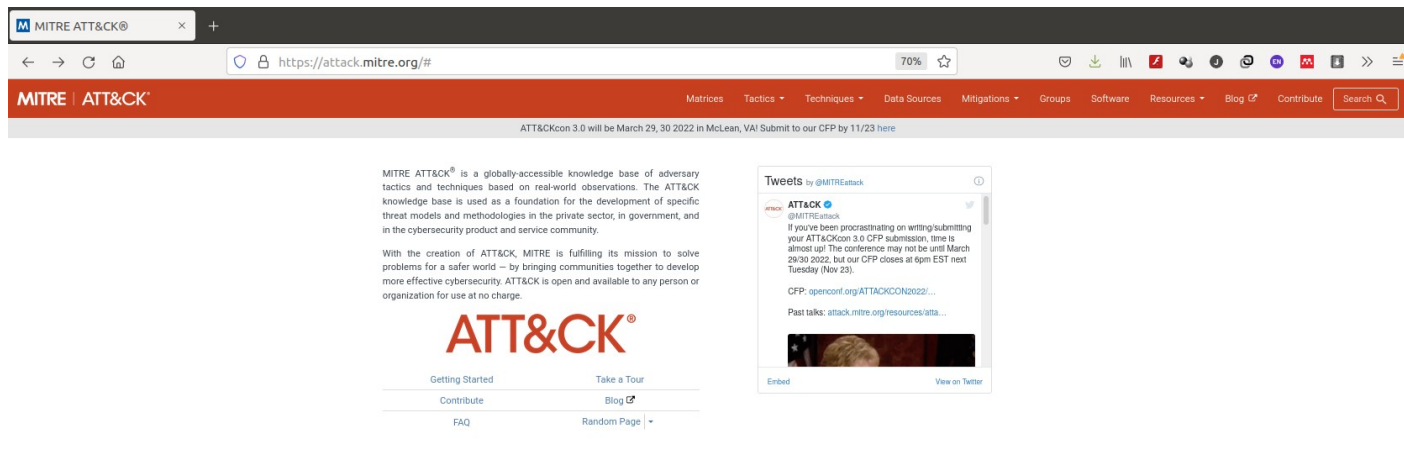
The screenshot shows the MITRE CVE website interface for CVE-2019-5432. The browser address bar shows the URL: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-5432>. The page features the CVE logo and navigation links such as CVE List, CNA, WG, Board, About, and News & Blog. A notice states: "Transition to the all-new CVE website at www.cve.org is underway and will last up to one year. (details)". The main content area displays the CVE ID "CVE-2019-5432" with a link to "Learn more at National Vulnerability Database (NVD)". The description reads: "A specifically malformed MQTT Subscribe packet crashes MQTT Brokers using the mqtt-packet module versions < 3.5.1, 4.0.0 - 4.1.3, 5.0.0 - 5.6.1, 6.0.0 - 6.1.2 for decoding." The references section includes a link to a HackerOne report: "MISC: <https://hackerone.com/reports/541354>". The assigning CNA is listed as "HackerOne". The date record created is "20190104". The phase is "Assigned (20190104)".

CVE-ID	
CVE-2019-5432	Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information	
Description	
A specifically malformed MQTT Subscribe packet crashes MQTT Brokers using the mqtt-packet module versions < 3.5.1, 4.0.0 - 4.1.3, 5.0.0 - 5.6.1, 6.0.0 - 6.1.2 for decoding.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
• MISC: https://hackerone.com/reports/541354	
Assigning CNA	
HackerOne	
Date Record Created	
20190104	Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20190104)	
Votes (Legacy)	
Comments (Legacy)	



Conceptos

- **Exploit** (MITRE ATT&CK - <https://attack.mitre.org/>)
 - Técnicas – tácticas – procedimientos (TTP)



ATT&CK Matrix for Enterprise

layout: flat ▾ show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	40 techniques	15 techniques	29 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques
Active Scanning (2) Batter Victim Host Information (4) Batter Victim Identity Information (3) Batter Victim Network Information (4) Batter Victim Org Information (4) Phishing for Information (18) Search Closed Sources (2) Search Open Technical Databases (5) Search Open Websites/Domains (2) Search Victim-Owned Websites	Acquire Infrastructure (6) Compromise Accounts (2) Compromise Infrastructure (6) Develop Capabilities (4) Establish Accounts (1) Establish Capabilities (4) Page Capabilities (2) Trusted Relationship Valid Accounts (4)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (2) Replication Through Removable Media Supply Chain Compromise (2) Trusted Relationship Valid Accounts (4)	Command and Scripting Interpreter (4) Container Administration Command Deploy Container Exploitation for Client Execution Live-Process Communication (2) Native API Scheduled Task/Job (4) Shared Modules Software Deployment Tools System Services (2) Task Execution (2)	Account Manipulation (4) BITS Jobs Boot or Logon Autostart Execution (15) Boot or Logon Initialization Scripts (5) Browser Extensions Compromise Client Software Binary Create Account (2) Create or Modify System Process (4) Event Triggered Execution (15) External Remote Services	Abuse Elevation Control Mechanism (4) Access Token Manipulation (2) Boot or Logon Autostart Execution (15) Boot or Logon Initialization Scripts (5) Create or Modify System Process (4) Domain Policy Modification (2) Domain Policy Modification (2) Escape to Host Event Triggered Execution (15) Exploitation for Privilege Escalation	Abuse Elevation Control Mechanism (4) BITS Jobs Build Image on Host Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Domain Policy Modification (2) Execution Guardrails (1) File and Directory Permissions Modification (2) Hide Artifacts (4)	Adversary-in-the-Middle (2) Brute Force (4) Credentials from Password Stores (2) Exploitation for Credential Access Forged Web Credentials (2) Input Capture (4) Network Sniffing OS Credential Dumping (2)	Account Discovery (4) Application Window Discovery Browser Bookmark Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Storage Object Discovery Container and Resource Discovery Domain Trust Discovery File and Directory Discovery Group Policy Discovery Network Service Scanning Network Share Discovery	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (2) Remote Services (2) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (4)	Adversary-in-the-Middle (2) Archive Collected Data (2) Automated Collection Browser Session Hijacking Clipboard Data Data from Cloud Storage Object Data from Configuration Repository (2) Data from Information Repositories (2) Data from Local System	Application Layer Protocol (4) Communication Through Removable Media Data Encoding (2) Data Obfuscation (2) Dynamic Resolution (2) Exfiltration Over C2 Channel Exfiltration Over Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling	Automated Exfiltration (1) Data Transfer Size Limits Data Manipulation (2) Exfiltration Over Alternative Protocol (2) Exfiltration Over Network Medium (2) Exfiltration Over Physical Medium (2) Exfiltration Over Web Service (2) Scheduled Transfer Transfer Data to Cloud	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (2) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop



Conceptos

- **Exploit** (MITRE ATT&CK - <https://attack.mitre.org/>)
 - **Matrices** (<https://attack.mitre.org/matrices/enterprise/>)

The screenshot displays the MITRE ATT&CK Enterprise Matrix page. The page header includes the MITRE logo and the text "Matrix - Enterprise | MITRE". The browser address bar shows the URL <https://attack.mitre.org/matrices/enterprise/>. The page content is organized into a grid of 13 categories, each with a list of attack techniques. The categories are: Reconnaissance (13 techniques), Resource Development (13 techniques), Initial Access (13 techniques), Execution (13 techniques), Persistence (13 techniques), Privilege Escalation (13 techniques), Defense Evasion (13 techniques), Credential Access (13 techniques), Discovery (13 techniques), Lateral Movement (13 techniques), Collection (13 techniques), Command and Control (13 techniques), Exfiltration (13 techniques), and Impact (13 techniques). Each category contains a list of techniques with their IDs and names. For example, under Reconnaissance, techniques include T1590 (System Discovery), T1591 (System Discovery), T1592 (System Discovery), T1593 (System Discovery), T1594 (System Discovery), T1595 (System Discovery), T1596 (System Discovery), T1597 (System Discovery), T1598 (System Discovery), T1599 (System Discovery), T1600 (System Discovery), T1601 (System Discovery), and T1602 (System Discovery). The page also includes a sidebar with navigation links for different matrix types (Enterprise, PRE, Windows, macOS, Linux, Cloud, Network, Containers, Mobile, IoT) and a search bar at the top right.

<https://attack.mitre.org/techniques/T1578>



Conceptos

- **Exploit (MITRE ATT&CK - <https://attack.mitre.org/>) - Ejemplo**
 - CVE-2017-0144 (smb-eternalblue)
 - TA: Lateral Movement
 - Tech: Exploitation of Remote Services
 - Software: InvisiMole y Lucifer

The screenshot shows the MITRE ATT&CK website. The 'Techniques' page is displayed, with the 'Exploitation of Remote Services' category selected. The 'InvisiMole' technique is highlighted, showing its ID (S0260), name, and description. The description states: 'InvisiMole is a module system program that has been used by the InvisiMole Group since at least 2013. InvisiMole has two backdoor modules called RC2FM and RC2CL, that are used to perform post-exploitation activities. It has been discovered on compromised victims in the Ukraine and Russia. Garmendy Group infrastructure has been used to download and execute InvisiMole against a small number of victims.' The 'Techniques Used' table is also visible, showing the domains, IDs, names, and uses of the techniques used by InvisiMole.

The screenshot shows the MITRE ATT&CK website. The 'Software' page for InvisiMole is displayed. The page shows the ID (S0260), type (MALWARE), platforms (Windows), contributors (ESET), version (2.0), created date (17 October 2018), and last modified date (21 October 2020). The 'Techniques Used' table is also visible, showing the domains, IDs, names, and uses of the techniques used by InvisiMole.

The screenshot shows the MITRE ATT&CK website. The 'Software' page for Lucifer is displayed. The page shows the ID (S0532), type (MALWARE), platforms (Windows), contributors (Denys Nisem, BT Security), version (1.1), created date (16 November 2020), and last modified date (01 October 2021). The 'Techniques Used' table is also visible, showing the domains, IDs, names, and uses of the techniques used by Lucifer.



Conceptos

- **Mitigación**

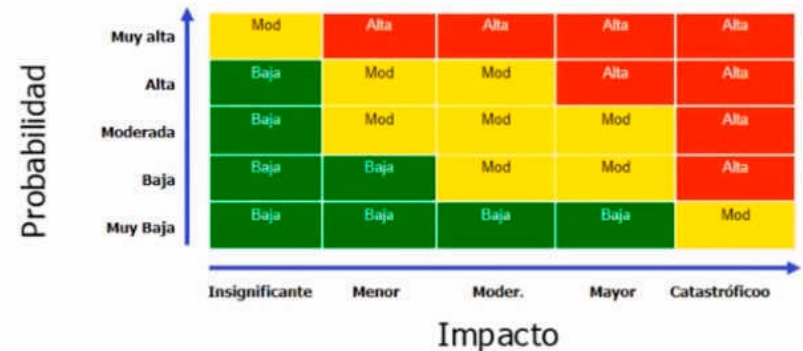
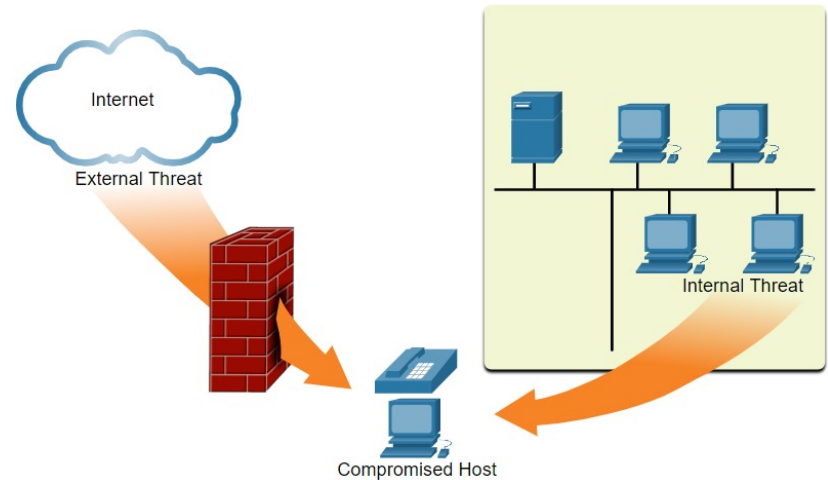
- La mitigación es la **contra-medida** que reduce la probabilidad o la severidad de una posible amenaza o riesgo. La seguridad de redes consiste en técnicas de mitigación múltiples.

- **Riesgo**

- El riesgo es la **probabilidad** de que una amenaza explote la vulnerabilidad de un activo, con el objetivo de afectar negativamente a una organización. El riesgo se mide utilizando la probabilidad de ocurrencia de un evento y sus consecuencias.

- **Vector de ataque**

- Un vector de ataque es una **ruta** por la cual un atacante puede obtener acceso a un servidor, host o red. Los vectores de ataque se originan dentro o fuera de la red corporativa.



Conceptos

- **Pérdida/Filtración de datos (I)**

- Términos utilizados para describir cuándo los datos se pierden con o sin intención, son robados o se filtran fuera de la organización. La pérdida de datos puede generar:

- Daño de la marca/pérdida de la reputación.
 - Pérdida de la ventaja competitiva.
 - Pérdida de clientes.
 - Pérdida de ingresos.
 - Acciones legales que generen multas y sanciones civiles.
 - Costo y esfuerzo significativos para notificar a las partes afectadas y recuperarse de la transgresión.



Conceptos

- **Pérdida/Filtración de datos (II)**

- Vectores de pérdida de datos

- Correo electrónico / Redes sociales: El correo electrónico o los mensajes de mensajería instantánea interceptados podrían capturarse y descifrar el contenido.
 - Dispositivos no encriptados: Si los datos no se almacenan utilizando un algoritmo de cifrado, entonces el ladrón puede extraer datos confidenciales de valor.
 - Dispositivos de almacenamiento en la nube: Los datos confidenciales se pueden perder si el acceso a la nube se ve comprometido debido a ajustes débiles en la seguridad.
 - Medios extraíbles: Un riesgo es que un empleado pueda realizar una transferencia no autorizada de datos a un dispositivo USB. Otro riesgo es que el dispositivo USB que contiene datos corporativos de valor se puede extraviar.
 - Respaldo físico: Los datos confidenciales deben triturarse cuando ya no sean necesarios.
 - Control de Acceso Incorrecto: Las contraseñas o contraseñas débiles que se hayan visto comprometidas pueden proporcionar al atacante un acceso fácil a los datos corporativos.

Conceptos

- **Hacker (I)**

- Término usado para describir un atacante. Hay varios tipos:
 - Hackers de Sombrero Blanco: Son hackers éticos que utilizan sus habilidades de programación para fines buenos, éticos y legales. Las vulnerabilidades en la seguridad se informan a los desarrolladores para que las corrijan antes de que las vulnerabilidades puedan aprovecharse.
 - Hackers de Sombrero Gris: Son personas que cometen delitos y hacen cosas probablemente poco éticas, pero no para beneficio personal o ni para causar daños. Un hacker de sombrero gris puede divulgar una vulnerabilidad de la organización afectada después de haber puesto en peligro la red.
 - Hackers de sombrero negro: Son delincuentes poco éticos que violan la seguridad de una computadora y una red para beneficio personal o por motivos maliciosos, como ataques a la red.



Conceptos

- **Hacker (II)**

- Otros tipos:

- Script kiddies: Estos son adolescentes o hackers inexpertos que corren scripts, ejecutan herramientas y exploits existentes para ocasionar daño, pero generalmente no para obtener ganancias.
 - Agentes de Vulnerabilidad: Son generalmente hackers de sombrero gris que intentan descubrir los exploits e informarlos a los proveedores, a veces a cambio de premios o recompensas. (BugBounty - <https://www.facebook.com/whitehat> - <https://infogram.com/cazarrecompensas-de-bugs-informaticos-1g57pryy89ev201>)
 - Hacktivistas: Estos son hackers de sombrero gris que protestan en público contra las organizaciones o gobiernos mediante la publicación de artículos, videos, la filtración de información confidencial y la ejecución de ataques a la red.
 - Delincuentes cibernéticos: Son hackers de sombrero negro independientes o que trabajan para grandes organizaciones de delito cibernético.
 - Patrocinados por el estado: Son hackers de sombrero blanco o sombrero negro que roban secretos de gobierno, recopilan inteligencia y sabotean las redes. Sus objetivos son los gobiernos, los grupos terroristas y las corporaciones extranjeras. La mayoría de los países del mundo participan en algún tipo de hacking patrocinado por el estado.

Conceptos

- **Malware:**

- Se llama malware, del inglés malicious software, programa malicioso, programa maligno, badware, código maligno, software maligno, software dañino o software malintencionado a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.
- Tipos (I):
 - **Virus (I)**: requieren una acción humana para propagarse e infectar otros equipos. Cuando se abre, el virus se ejecuta e infecta el equipo.
 - Los virus pueden:
 - » Modificar, dañar, eliminar archivos o borrar discos duros completos.
 - » Causar problemas de arranque del equipo y dañar aplicaciones.
 - » Capturar y enviar información confidencial a los atacantes.
 - » Acceder a cuentas de correo electrónico y utilizarlas para propagarse.
 - » Permanecer inactivo hasta que el atacante lo requiera.

Conceptos

- **Malware:**
 - Tipos (II):
 - **Virus (II)** Tipos de virus:
 - Virus en el sector de arranque: El virus ataca el sector de arranque, la tabla de particiones de archivos o el sistema de archivos.
 - Virus de firmware: El virus ataca el firmware del dispositivo.
 - Virus de macros: El virus utiliza la función de macros de MS Office con fines maliciosos.
 - Virus del programa: El virus se introduce en otro programa ejecutable.
 - Virus de script: El virus ataca al intérprete del SO que se utiliza para ejecutar los scripts.

Conceptos

- **Malware:**

- Tipos (III):

- **Caballo de Troya:** Un Troyano es un programa que parece útil pero también transporta código malicioso. Tipos:
 - Acceso remoto: El Troyano activa el acceso remoto no autorizado.
 - Envío de datos: El Troyano le proporciona al atacante datos confidenciales, como contraseñas.
 - Destruutivo: El Troyano daña o elimina archivos.
 - Proxy: El Troyano usará el equipo de la víctima como dispositivo de origen para lanzar ataques y realizar otras actividades ilegales.
 - FTP: El Troyano habilita servicios no autorizados de transferencia de archivos en dispositivos finales.
 - Desactivador de software de seguridad: El Troyano detiene el funcionamiento de los programas antivirus o firewall.
 - Denegación de servicio (DoS): Caballo de Troya de DoS: retarda o detiene la actividad de red.
 - Keylogger: El Troyano intenta activamente robar información confidencial, como números de tarjetas de crédito, registrando las pulsaciones de teclas efectuadas en un formulario web.

Conceptos

- **Malware:**

- Tipos (IV):

- **Adware:** se suele distribuir en las descargas de software. Puede mostrar anuncios no solicitados mediante ventanas emergentes del navegador web, nuevas barras de herramientas o redireccionamientos inesperados a un sitio web diferente
 - **Ransomware:** cifra los archivos de la PC para que el usuario no pueda acceder a ellos y luego presenta un mensaje donde se exige un rescate para suministrar la clave de descifrado.
 - **Rootkit:** obtención de acceso a nivel de cuenta de administrador a un PC. Pueden alterar el firewall, la protección antivirus, los archivos del sistema e incluso los comandos del SO para ocultar su presencia. Pueden proveer una puerta trasera para que los atacantes accedan al equipo, carguen archivos e instalen nuevo software para utilizarlo en un ataque DDOS.
 - **Spyware:** Es similar al adware, pero se utiliza para recopilar información sobre el usuario y enviarla sin su consentimiento a los atacantes.
 - **Gusano:** Es un programa que se replica a sí mismo y se propaga automáticamente sin participación del usuario, al aprovechar vulnerabilidades de software legítimo. Utiliza la red para buscar otras víctimas con la misma vulnerabilidad. El objetivo de los gusanos suele ser quitar velocidad o interrumpir las operaciones de redes.

Conceptos

- Decálogo básico de ciberseguridad



Principios y recomendaciones básicas en CIBERSEGURIDAD

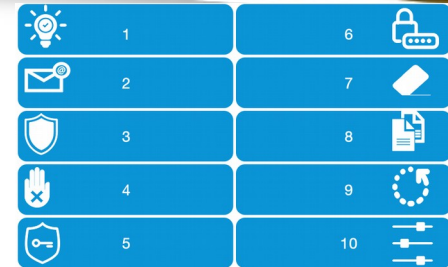
Decálogo Básico de Seguridad

Este decálogo de buenas prácticas pretende sentar las bases para establecer una cultura de seguridad.



 1	6 
 2	7 
 3	8 
 4	9 
 5	10 

Conceptos



- **Decálogo básico de ciberseguridad**

- I. La cultura de la ciberseguridad, la concienciación del empleado, debe ser uno de los pilares en lo que se asiente la ciberseguridad de cualquier Organización.
- II. No abrir ningún enlace ni descargar ningún fichero adjunto procedente de un correo electrónico que presente cualquier indicio o patrón fuera de lo habitual.
- III. Utilizar software de seguridad, herramientas antivirus y antimalware, cortafuegos personales, herramientas de borrado seguro, etc. debe ser algo irrenunciable cuando se utiliza un sistema de las TIC.
- IV. Limitar la superficie de exposición a las amenazas, no solo hay que implementar medidas de seguridad que protejan el acceso a la información, sino que hay que determinar los servicios que son estrictamente necesarios.
- V. Cifrar la información sensible, no hay otra alternativa.
- VI. Utilizar contraseñas adaptadas a la funcionalidad siendo conscientes de que la doble autenticación ya es una necesidad.
- VII. Hacer un borrado seguro de la información una vez que esta ya no sea necesaria o se vaya a retirar de uso el soporte en cuestión.
- VIII. Realizar copias de seguridad periódicas, no existe otra alternativa en caso de infección de código malicioso tipo ransomware, pérdida de datos, averías del hardware de almacenamiento, borrado de información involuntaria por parte del usuario, etc.
- IX. Mantener actualizadas las aplicaciones y el sistema operativo es la mejor manera de evitar dar facilidades a la potencial amenaza.
- X. Revisa regularmente la configuración de seguridad aplicada, los permisos de las aplicaciones y las opciones de seguridad.

Conceptos

- **Diferentes sectores de ciberseguridad:**
 - Detección de incidentes, inteligencia de amenazas, dark web, intrusiones, SIEM (security information and event management)
 - Análisis de incidentes, fraude y forense
 - Respuesta a incidentes, gestión de crisis, mitigación y recuperación
 - Normativa, certificación, aseguramiento y cumplimiento legal
 - Seguridad de datos, tratamiento y cifrado
 - Formación y entrenamiento en ciberseguridad
 - Seguridad en la identidad, privilegios y control de acceso
 - Seguridad en aplicaciones, sistemas operativos y web
 - Seguridad en dispositivos móviles y apps
 - Seguridad en desarrollo de Software y DevOps
 - Seguridad en servicios en la nube
 - Seguridad en las comunicaciones y redes, IPS, firewalls
 - Seguridad en infraestructuras OT e IoT

Conceptos

- Certificaciones**

Security Certification Progression Chart 2020

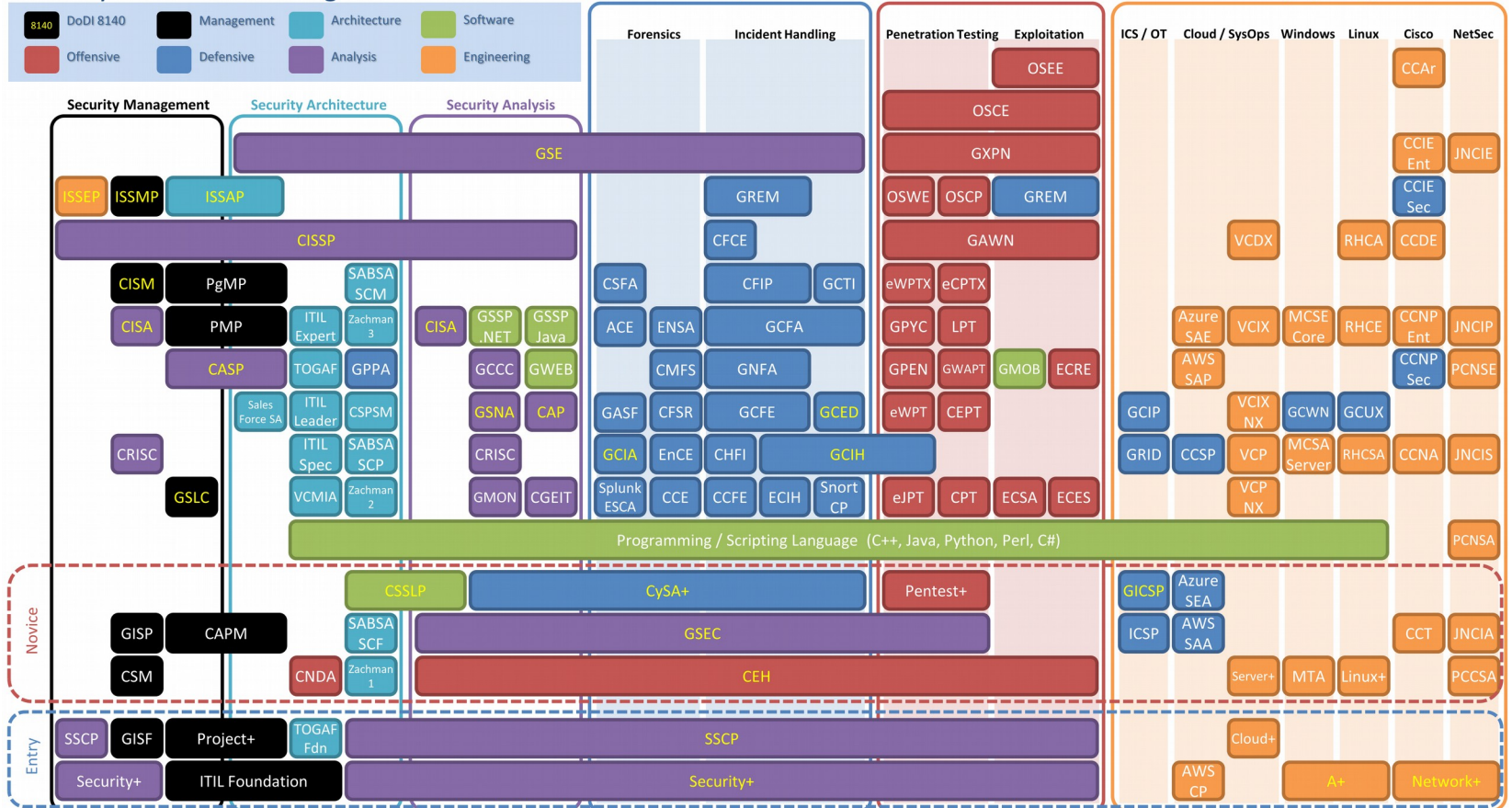


Tabla de contenidos

- Conceptos
- Seguridad de la Información
- IoT: Internet of Things

Seguridad de la Información

- Conceptos:
 - **Información:**
 - Hechos o ideas que pueden ser representado o codificado de diversas formas.
 - Conocimiento (datos o instrucciones) en un medio que pueden ser comunicados entre entidades o sistemas.
 - **Seguridad de la Información:** Protección de la información o sistemas de información de accesos, uso, divulgación, interrupción, modificación o destrucción no autorizados con el fin de garantizar la confidencialidad, la integridad y la disponibilidad.
 - **Controles de seguridad:** Control del manejo, operacional o técnico prescrito por un sistema para proteger la confidencialidad, integridad y disponibilidad del sistema o su información.

Seguridad de la Información

- Pilares de la seguridad de la información (CIA - inglés):
 - **Confidencialidad (C)**: Solamente individuos, entidades o procesos autorizados pueden tener acceso a información confidencial. Uso de algoritmos de cifrado criptográfico para cifrar y descifrar datos Ej: AES, RSA, 3DES, ...
 - **Integridad (I)**: Se refiere a proteger los datos de modificaciones no autorizadas. Uso de algoritmos de hashing criptográficos. Ej: SHA, MD5, ...
 - **Disponibilidad (A)**: Los usuarios autorizados deben tener acceso ininterrumpido a los recursos y datos importantes. Requiere implementar servicios puertas de enlace y enlaces redundantes.

Seguridad de la Información

- Otros conceptos igualmente importantes (Guía de Gestión de Riesgos, INCIBE):
 - **Autenticidad:** La información es lo que dice ser o el transmisor de la información es quien dice ser.
 - **No repudio:** Estrechamente relacionado con la Autenticidad. Permite, en caso de ser necesario, que sea posible probar la autoría u origen de una información.



Seguridad de la Información

- Elementos de la seguridad de la información (NIST-SP-800-12r1)
 - La seguridad de la información apoya la misión de la organización.
 - La seguridad de la información es un elemento integral de la buena gestión.
 - Las protecciones de la seguridad de la información se aplican de forma proporcional al riesgo.
 - Las funciones y responsabilidades en materia de seguridad de la información se hacen explícitas.
 - Las responsabilidades de seguridad de la información de los propietarios de sistemas van más allá de su propia organización.
 - La seguridad de la información requiere un enfoque global e integrado.
 - La seguridad de la información se evalúa y supervisa regularmente.
 - La seguridad de la información está limitada por factores sociales y culturales.

Seguridad de la Información

- Riesgos: Las amenazas sobre la información almacenada en un sistema informático. Ejemplos:
 - De **origen natural**: inundaciones, terremotos, incendios, rayos
 - **Fallos de la infraestructura auxiliar**: fallos de suministro eléctrico, refrigeración, contaminación...
 - **Fallos de los sistemas informáticos y de comunicaciones**: fallos en las aplicaciones, hardware o equipos de transmisiones
 - **Error humano**: errores accidentales o deliberados de las personas que interactúan con la información

Seguridad de la Información

- Efectos de los ataques sobre la información:
 - **Interrupción:** se produce cuando un recurso, herramienta o la propia red deja de estar disponible debido al ataque.
 - **Intercepción:** se logra cuando un tercero accede a la información del ordenador o a la que se encuentra en tránsito por la red.
 - **Modificación:** se trata de modificar la información sin autorización alguna.
 - **Fabricación:** se crean productos, tales como páginas web o tarjetas magnéticas falsas.

Seguridad de la Información

- Clasificación de incidentes (INCIBE-CERT)

Nivel	Clasificación	Nivel	Clasificación
Crítico	APT / Ciberterrorismo	Medio	Contenido abusivo
	Código dañino		Obtención de información
	Intrusión		Intento de intrusión
	Disponibilidad		Fraude
Muy alto	Contenido abusivo	Bajo	Vulnerabilidad
	Código dañino		Intrusión sin privilegios
	Intrusión		Otros
	Compromiso de la información		
Alto			

Seguridad de la Información

- Mecanismos de defensa:
 - **Firewall**: sistemas de restricción de tráfico basado en reglas.
 - **Sistemas IDS / IPS**: sistemas de monitorización, detección y/o prevención de accesos no permitidos en una red.
 - **Honeypot**: equipos aparentemente vulnerables diseñados para atraer y detectar a los atacantes, protegiendo los sistemas realmente críticos.
 - **SIEM**: sistemas de correlación de eventos y generación de alertas de seguridad.
 - **Antimalware**: sistemas de detección de malware informático.

Seguridad de la Información

- Roles y responsabilidades (INCIBE)
 - **CISO (Chief Information Security Officer)** es el director de seguridad de la información. Básicamente es un rol desempeñado a nivel ejecutivo y su función principal es la de alinear la seguridad de la información con los objetivos de negocio. De esta forma se garantiza en todo momento que la información de la empresa está protegida adecuadamente.

RESPONSABILIDADES:

- Generar e implantar políticas de seguridad de la información.
- Garantizar la seguridad y privacidad de los datos.
- Supervisar la administración del control de acceso a la información.
- Supervisar el cumplimiento normativo de la seguridad de la información.
- Responsable del equipo de respuesta ante incidentes de seguridad de la información de la organización.
- Supervisar la arquitectura de seguridad de la información de la empresa.

Seguridad de la Información

- Roles y responsabilidades (INCIBE)
 - **CSO (Chief Security Officer)** es el responsable de la seguridad de la organización. Al CSO a veces se le denomina responsable de seguridad corporativa. Comparándolo con el CISO, el rol del CISO suele estar más centrado en aspectos de seguridad de la información, mientras que al CSO tiene las siguientes:

RESPONSABILIDADES:

- Tener una visión de negocio que comprenda los riesgos que afronta la organización y cómo tratarlos.
- Entender la misión y los objetivos de la empresa y asegurarse de que todas las actividades son planificadas y ejecutadas para satisfacer dichos objetivos.
- Comprender las necesidades normativas, la gestión de la reputación de la organización y las expectativas de los usuarios.
- Establecer los planes de continuidad de negocio y recuperación de desastres en el ámbito de las tecnologías de la información.
- Estar al tanto de los cambios normativos, debiendo informarse de las consecuencias para las actividades de la organización y proponiendo las medidas oportunas para adecuarse al nuevo marco normativo.

Cuando existen CSO y CISO, el CISO reporta al CSO y el CSO a la dirección.

Seguridad de la Información

- Roles y responsabilidades (INCIBE)
 - **CEO (Chief Executive Officer)** es el director ejecutivo, el gerente, el cargo más alto dentro del organigrama de la organización. Es el responsable final de las acciones que se lleven a cabo dentro de la empresa, de su desempeño y su eficiencia.
 - Su función principal es la de supervisar y velar porque la estrategia definida en la empresa cumpla con la consecución de los objetivos de la organización, además de sembrar los principios y pilares básicos a seguir dentro de la empresa.
 - El CEO tiene una importante relación con el CIO, debido a que las estrategias de las empresas están estrechamente ligadas al ámbito de las tecnologías de la información.

Seguridad de la Información

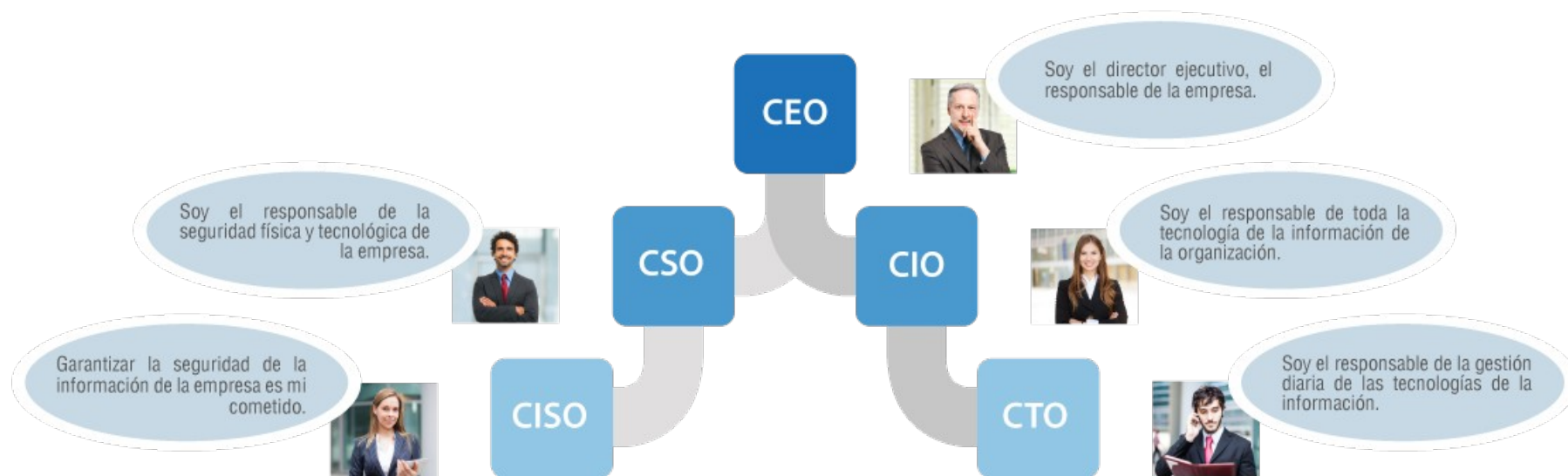
- Roles y responsabilidades (INCIBE)
 - **CIO (Chief Information Officer)** es el gerente de sistemas o director de tecnologías de la información. Reporta directamente al CEO, y se encarga básicamente de que las estrategias de la organización estén alineadas con la tecnología de la información para lograr los objetivos planificados.
 - Se encarga de mejorar los procesos de tecnologías de la información de la organización, gestionar el riesgo y la continuidad de negocio, controlar el coste en infraestructura de tecnologías de la información, alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos, y establecer mejoras e innovaciones de soluciones y productos.

Seguridad de la Información

- Roles y responsabilidades (INCIBE)
 - **CTO (Chief Technology Officer)** en un rol similar al CIO pero más técnico. Se entremezclan con las funciones de los CIO. Sin embargo podemos decir que es un director técnico, siendo su responsabilidad la gestión del día a día de las tecnologías de la información.

Seguridad de la Información

- Roles y responsabilidades (INCIBE)



Seguridad de la Información

- Roles y responsabilidades (NIST SP 800-12r1)
 - **Risk Executive Function (Senior Management) - Función Ejecutiva de Riesgos (Alta Dirección):** persona o grupo de personas (consejo administración, director general, director de información responsable de garantizar:
 - RESPONSABILIDADES:
 - Definir un enfoque holístico para abordar el riesgo en toda la organización;
 - Desarrollar una estrategia de gestión de riesgos en la organización de forma coherente y que refleje la tolerancia al riesgo y tipos de riesgo para garantizar el éxito de la empresa;
 - Apoyar el intercambio de información entre los encargados de la autorización y otros líderes de alto nivel dentro de la organización;
 - Supervisar las actividades relacionadas con la gestión de riesgos en toda la organización.

Seguridad de la Información

- Roles y responsabilidades (NIST SP 800-12r1)
 - **System Security Engineer (SSE)** persona, grupo u organización responsable de llevar a cabo actividades de ingeniería de seguridad de sistemas.
 - RESPONSABILIDADES:
 - Diseñar y desarrollar sistemas organizativos o actualizar sistemas heredados; y
 - Coordinar las actividades relacionadas con la seguridad con los arquitectos de seguridad de la información de la agencia, los propietarios del sistema, los proveedores de control común y los responsables de seguridad del sistema.

Seguridad de la Información

- Roles y responsabilidades (NIST SP 800-12r1)
 - **Administrador del sistema** es un individuo, grupo u organización responsable de configurar y mantener un sistema o componentes específicos de un sistema.
 - RESPONSABILIDADES:
 - Instalar, configurar y actualizar el hardware y el software;
 - Establecer y gestionar las cuentas de usuario;
 - Supervisar las tareas de copia de seguridad y recuperación;
 - Implementación de controles técnicos de seguridad.

Seguridad de la Información

- Roles y responsabilidades (NIST SP 800-12r1) (otros)
 - **Auditor** responsables de examinar los sistemas para determinar si el sistema cumple con los requisitos de seguridad establecidos y las políticas de la organización y si los controles de seguridad son adecuados. Las auditorías informales pueden ser realizadas por quienes operan el sistema que se está examinando o por terceros auditores imparciales
 - **Personal de seguridad física** responsable de desarrollar y aplicar los controles de seguridad física adecuados. Se ocupa de las instalaciones del sistema central, las instalaciones de reserva y los entornos de oficina.

Tabla de contenidos

- Conceptos
- Seguridad de la Información
- **IoT: Internet of Things**

Internet of Things (IoT)

- **Elementos de IoT:**
 - Cosas (Things): objeto físico o virtual capaz de ser identificado e integrado en redes de comunicación.
 - Capacidad de comunicación
 - Opcional: capacidad de detectar y capturar datos, actuar, almacenar y procesar datos...
 - Gestionados por sistemas inteligentes capaces de conectarse a las cosas para monitorizarlas y controlarlas
 - Toma de decisiones: simples como umbrales, o avanzadas como aprendizaje automático.
 - Información analizada y procesada localmente (edge) o en la nube (cloud computing)
 - Sensores y actuadores:
 - Sensores: medir indicadores físicos, químicos, biológicos, ... para generar datos cuantitativos asociados.
 - Actuador: entidad responsable de mover o controlar un sistema o mecanismo.

Internet of Things (IoT)

- Sistemas integrados/empotrados/embebidos (embeded): en la mayoría de los despliegues IoT, los sensores y actuadores no están aislados, sino integrados en sistemas.
 - También pueden/suelen tener capacidades para conectarse a una LAN, la nube, capacidad de ejecutar software, ...
 - Ej: implantes médicos, relojes inteligentes, ...

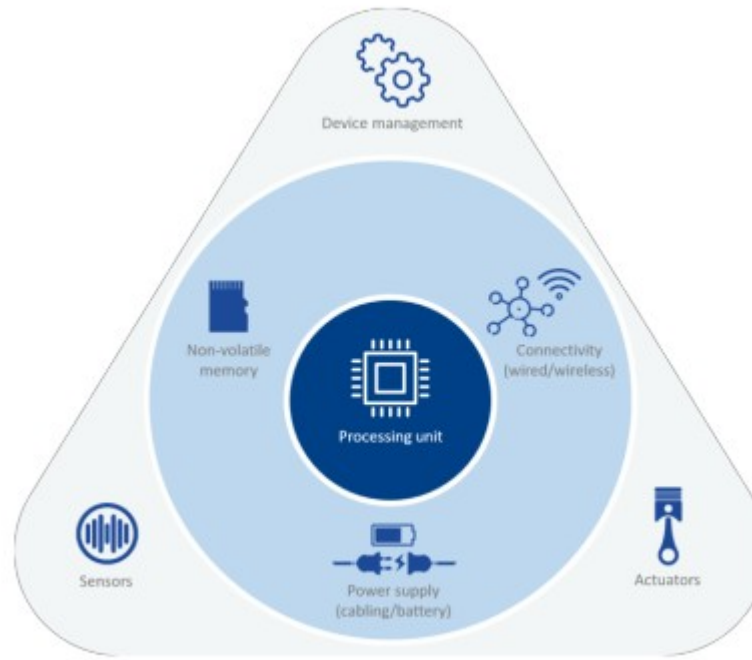


Figure 3: Structure of an IoT embedded system



Internet of Things (IoT)

- Comunicaciones: diferentes protocolos en diferentes ecosistemas y pasarelas que garantizan la interoperabilidad.
 - Ej: ZigBee, Bluetooth (BLE), Wifi, NFC, RFID, redes móviles, LoRaWan, SigFox, NB-IoT, Ethernet, USB, ...

SESSION		AMQP, CoAP, DDS, MQTT, XMPP
NETWORK	ENCAPSULATION	6LowPAN, Thread
	ROUTING	CARP, RPL
DATALINK		Bluetooth / BLE, Wi-Fi / Wi-Fi HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB

Table 1: Indicative listing of communication protocols for IoT⁴⁶

Internet of Things (IoT)

- **Amenazas para las tecnologías emergentes (IoT)**

(<https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-sectorial-threat-analysis-ebook-en-es.pdf>)

COMPONENTES RELACIONADOS: GRUPOS DE ACTIVOS	EXPOSICIÓN A LAS AMENAZAS
Factor humano	Amenazas internas, problemas del trabajo en equipo, limitaciones internas, «hacktivismo», pérdida de servicios de respaldo, corte de servicios, cortes de red, modificaciones no intencionadas, sabotaje, violación de reglas y normativas, infracción de la legislación, requisitos de contratos, incumplimiento de requisitos contractuales (p. ej., mantenimiento de programas informáticos), explotación de programas informáticos, ingeniería social, robo de identidades.
Diseño de los programas Informáticos	Amenazas internas, «hacktivismo», modificaciones no intencionadas, uso erróneo o administración incorrecta de dispositivos y sistemas, sabotaje, fallos en los procesos SDLC, fallos de terceros, incumplimiento de requisitos contractuales (p. ej., mantenimiento de programas informáticos), explotación de programas informáticos, pérdidas o filtración de información.

Internet of Things (IoT)

- **Características que dificultan la seguridad en dispositivos IoT:**
 - **Superficie de ataque muy grande:** grandes cantidades de datos procedentes de diversas fuentes.
 - **Recursos limitados de los dispositivos:** capacidades limitadas de procesamiento, memoria, energía, ... hacen “imposible” la aplicación de mecanismos de seguridad.
 - **Ecosistema complejo:** No es un conjunto de dispositivos independientes. Intervienen diversos dispositivos, comunicaciones, interfaces, personas, ...
 - **Fragmentación de normas y reglamentos:** Fragmentación y lentitud en generación y adopción de normas y reglamentos. “La tecnología avanza más rápido que las leyes”.
 - **Despliegue generalizado:** Tendencia de migración de sistemas incluso infraestructuras críticas (IC) a IoT.
 - **Integración de la seguridad:** Diferentes dispositivos y sistemas de IoT diversos hacen difícil su integración e interoperatividad.

Internet of Things (IoT)

- **Características que dificultan la seguridad en dispositivos IoT:**
 - **Aspectos de seguridad física:** Presencia de actuadores que actúan sobre el mundo físico.
 - **Bajo coste:** El bajo coste de los dispositivos suele asociarse con implicaciones en términos de seguridad, pasa a un segundo plano, se limitan la implementación de mecanismos de seguridad.
 - **Falta de experiencia:** Ámbito bastante novedoso, faltan personas con conocimientos y experiencia en ciberseguridad del IoT.
 - **Actualizaciones de seguridad:** Los diversos dispositivos e interfaces de usuario hacen muy difícil las actualizaciones. Lo más común son actualizaciones Over-The-Air (OTA) que también pueden ser inseguras.
 - **Programación insegura:** Más énfasis en la funcionalidad y la usabilidad que en la seguridad por limitaciones de tiempo y presupuesto,.
 - **Responsabilidades poco claras:** Amplia y compleja cadena de suministro de dispositivos IoT y herramientas para su fabricación. Ambigüedades en la asignación de responsabilidades.

Internet of Things (IoT)

- **Características que dificultan la seguridad en dispositivos IoT:**
 - **contraseñas débiles o embebidas:** posibilidad de obtener las contraseñas mediante un ataque por fuerza bruta, procesos de ingeniería inversa, ...
 - **Servicios de red inseguros:** se deben evitar aquellos servicios de red innecesarios o inseguros que se ejecutan en los dispositivos en segundo plano y que están expuestos a Internet.
 - **Interfaces inseguras en el ecosistema IoT:** las herramientas externas a los dispositivos como interfaces web, API en el backend o servicios en la nube pueden estar configurados de una manera insegura. Se debe adoptar medidas de control de acceso a dichas interfaces, filtrar las entradas y salidas de los servicios y asegurar las comunicaciones añadiendo algoritmos de encriptación son las medidas más efectivas para paliar el problema.
 - **Uso de componentes inseguros o desactualizados:** Componentes software y hardware inseguros u obsoletos, de terceros, de distintos fabricantes, ...
 - **Falta de seguridad en el almacenamiento y transferencia de datos:** Algoritmos de cifrado cuando se manejan datos sensibles. Control de acceso a los mismos dentro del ecosistema IoT.
 - **Inadecuada gestión de dispositivos:** Monitorización de los sistemas, políticas de desmantelamiento, borrado seguro de los dispositivos, ...
 - **Configuraciones por defecto inseguras.**
 - **Falta de bastionado físico:** Controles sobre el acceso físico al dispositivo.

Internet of Things (IoT)

- Taxonomía de activos en IoT

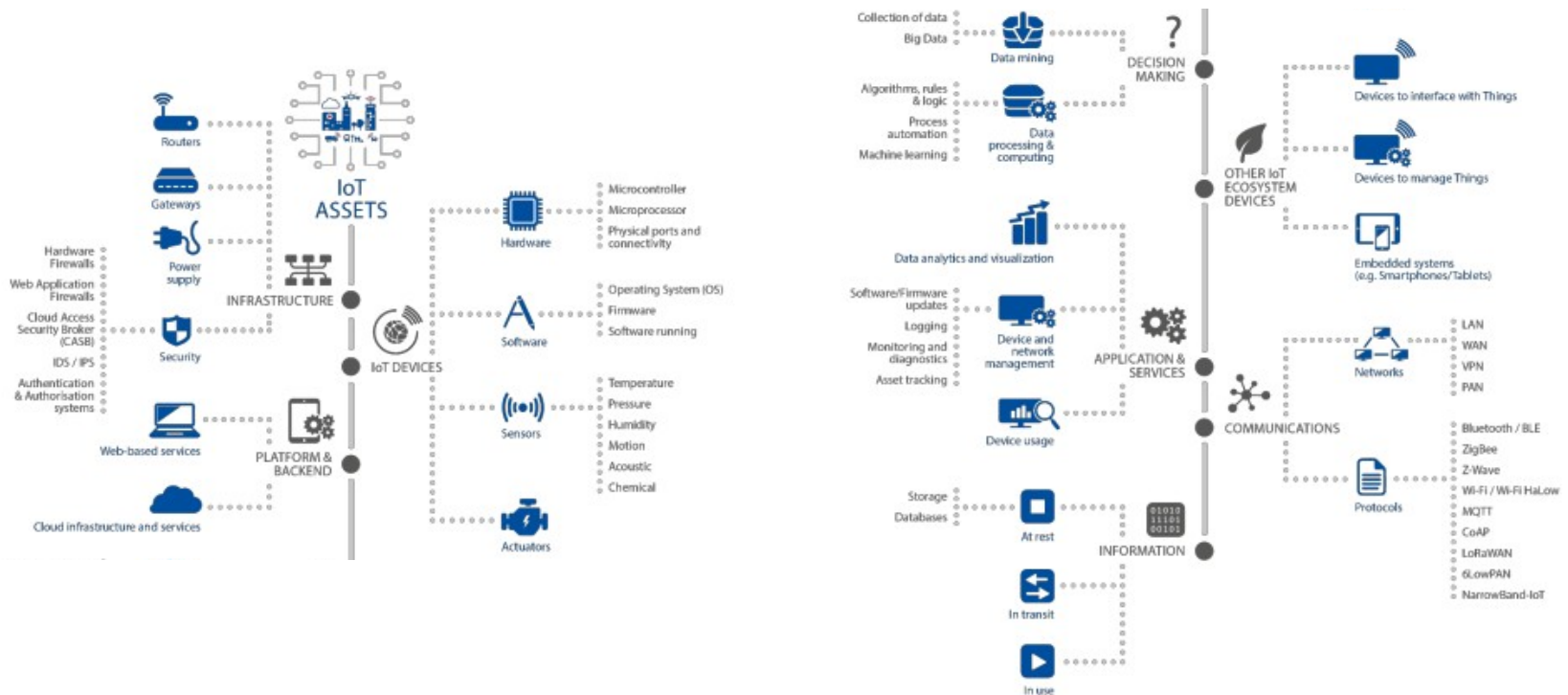


Figure 5: Asset taxonomy



Internet of Things (IoT)

- Impacto de las amenazas en IoT

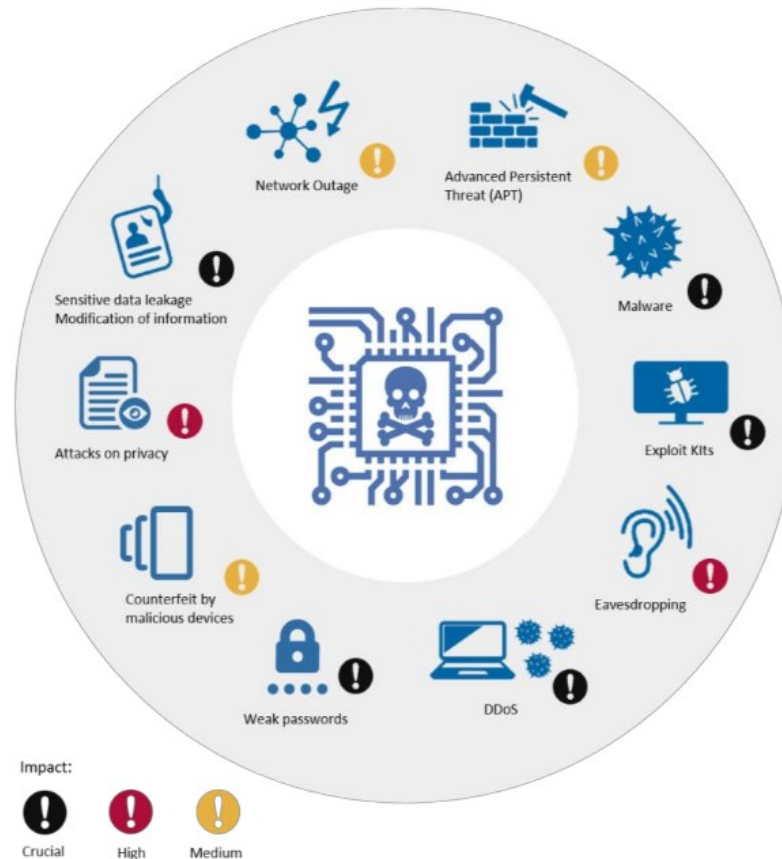


Figure 9: IoT threats impact

Internet of Things (IoT)

- Taxonomía de las amenazas en IoT

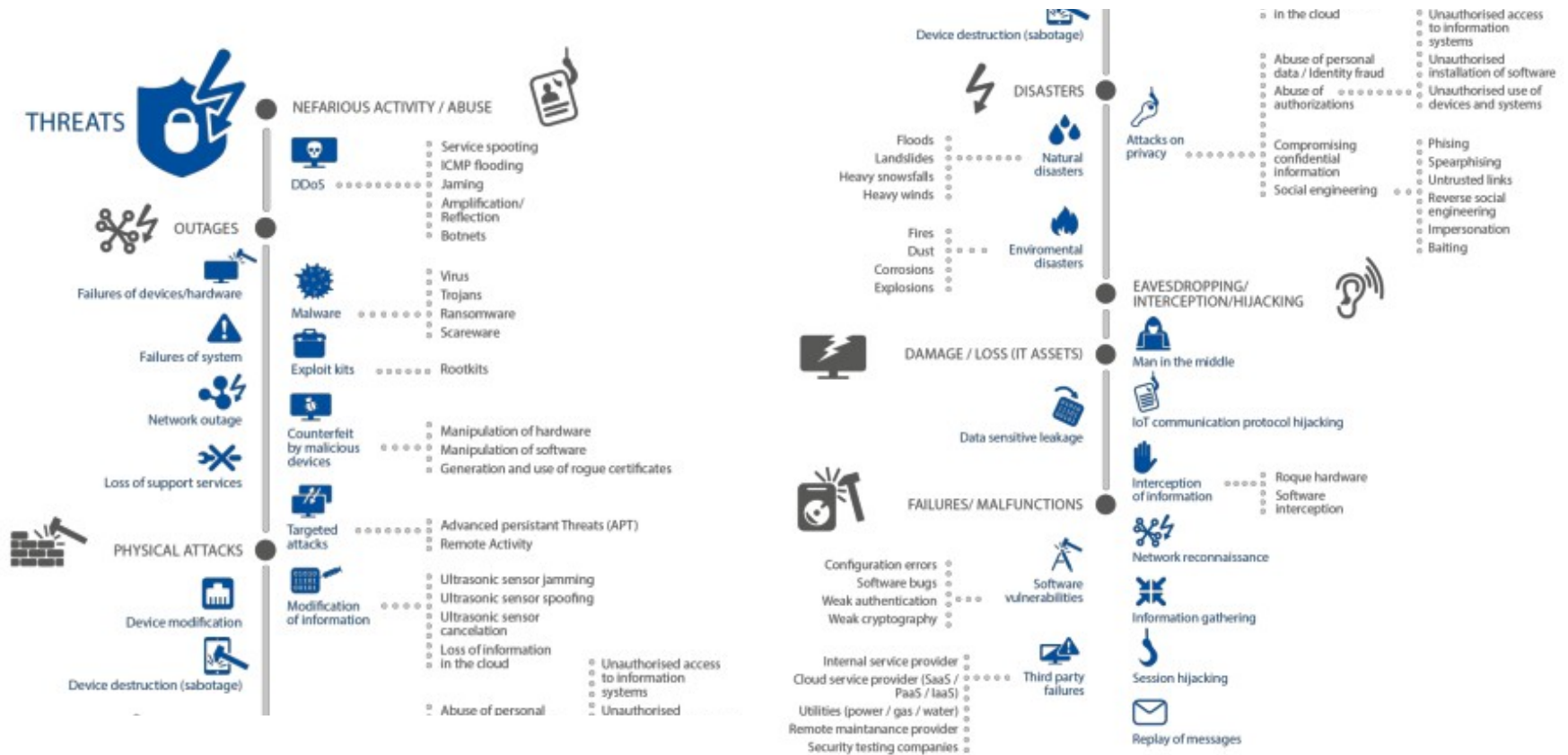
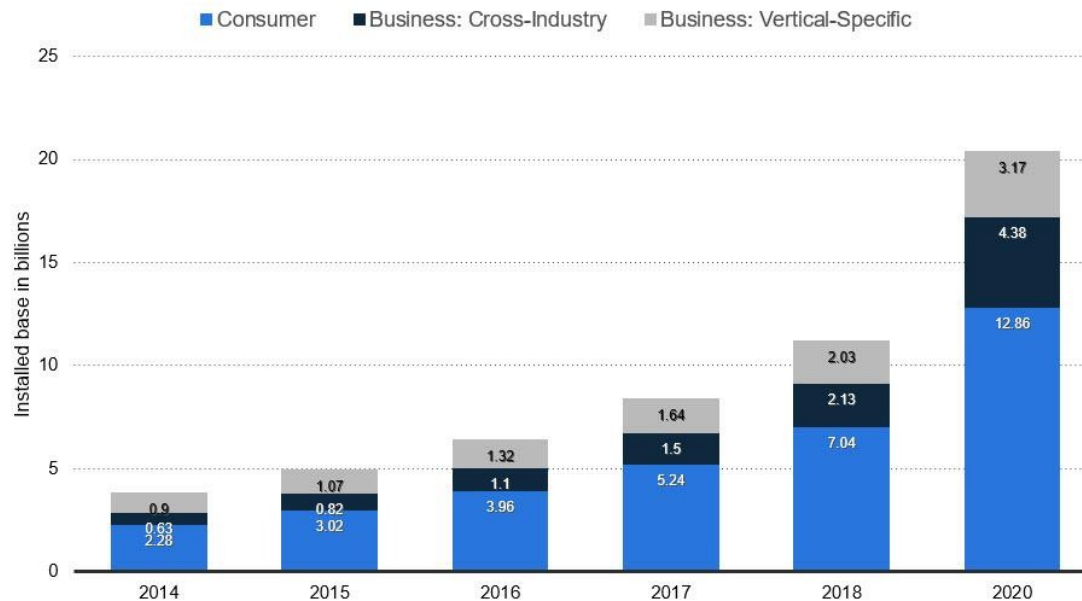


Figure 8: IoT Threat taxonomy



Internet of Things (IoT)

**The Internet of Things (IoT) Units Installed Base By Category
2014 to 2020 (in billions of units)**



statista



Internet of Things (IoT)

- Buenas Prácticas en Internet de las Cosas, IoT (CCN-CERT):**

Superficie de Ataque	Vulnerabilidad	Superficie de Ataque	Vulnerabilidad
Control de Acceso al Ecosistema	Confianza implícita entre todos los componentes del sistema. (In)Seguridad en el registro de componentes (<i>enrollment</i>). La retirada o jubilación de equipos (<i>decommissioning</i>). La pérdida de las credenciales y procedimientos de acceso.	Interfaces físicas del dispositivo	Extracción del Firmware. Interfaz de línea de comando de los usuarios y del Administrador. Posibilidades de escalado de privilegios. Borrado (<i>Reset</i>) a un estado inseguro. Extracción de los medios de almacenamiento. (No)Resistencia a las manipulaciones físicas del dispositivo. Presencia de puertos de depuración (p.ej., JTAG TM). Exposición de número de serie o la identidad del dispositivo.
Memoria del dispositivo	Nombres de usuario y contraseñas en claro. Credenciales de terceras partes en claro. Claves de cifrado en claro.	Interfaz Web del dispositivo	SQL injection, Cross-site scripting y Cross-site Request Forgery. Extracción y listado de nombres de usuarios válidos. La presencia de contraseñas débiles. Posibilidad de bloquear cuentas. Existencia de credenciales por defecto.
Servicios de red del dispositivo	Divulgación de información. Interfaz de línea para los usuarios y para el Administrador. Posibilidades de inyección de código. Denegación de servicio. La existencia de servicios no cifrados. El uso de cifrados mal implementados. Presencia de servicios de prueba y/o desarrollo no eliminados o no desactivados en escenarios de producción. Problemas de buffer overflow en el software. UPnP [®] y servicios UDP vulnerables. Las posibilidades de éxito en ataques DoS (<i>Denegation of Service</i>). La actualización On The Air (OTA) del Firmware del dispositivo. Las posibilidades de éxito de ataques de Replay. Falta de verificación de las cargas de datos o códigos. Falta de verificación de la integridad de los mensajes, tanto si son datos como comandos	El Firmware del dispositivo	Credenciales incrustadas en el código (<i>hardcoded credentials</i>). Divulgación de URL e información sensible. Presencia de claves de cifrado en claro. Alteración del cifrado en sí mismo (simétrico y asimétrico). Mostrar la versión del Firmware y/o la fecha de la última actualización. Cuentas olvidadas de usuario actuando como puertas traseras. Servicios vulnerables activos (web, ssh, tftp, etc.). Exposición de las API de seguridad del dispositivo. Posibilidad de retomar a una versión anterior insegura.

Internet of Things (IoT)

- Buenas Prácticas en Internet de las Cosas, IoT (CCN-CERT):**

Superficie de Ataque	Vulnerabilidad
Interfaz Administrativa	SQL injection, Cross-site scripting y Cross-site Request Forgery. Mecanismos de descubrimiento de nombres de usuario válidos. La presencia de contraseñas débiles y credenciales por defecto conocidas. La posibilidad de que se dé el bloqueo de cuentas. La ausencia de opciones de Seguridad/Cifrado y de <i>logging</i> seguro. La no autenticación con doble factor. La incapacidad para limpiar de forma segura el dispositivo (<i>wipe</i>).
Almacenamiento local de los datos	La presencia de datos no cifrados y/o el cifrado con claves comprometidas. La falta de controles de integridad de los datos. El uso de una misma clave de cifrado/descifrado de todos los datos.
Interfaz Web con la Nube	SQL injection, Cross-site scripting y Cross-site Request Forgery. El descubrimiento de nombres de usuario válidos. La presencia de contraseñas débiles y de credenciales por defecto. El posible bloqueo de cuentas. El no cifrado de lo que se transporta o comunica. La presencia de mecanismo de recuperación de claves y contraseñas que sea inseguro. La falta de autenticación de doble factor.
Backend API de terceras partes	Envío no cifrado de información personal o identificativa. El modo de cifrado de la información personal e identificativa. La divulgación de información interna del dispositivo. La divulgación de la ubicación del dispositivo.
Mecanismo de actualización	El que las actualizaciones se envíen sin cifrar. Que las actualizaciones no vengán correctamente firmadas. Que la URL de las actualizaciones sea modificable. Que no haya o sea ineficaz la verificación de las actualizaciones, o la falta de autenticación de las mismas. La posibilidad de instalar actualizaciones maliciosas. La pérdida temporal o definitiva del mecanismo de actualización. La ausencia de un mecanismo manual de actualización.
Aplicación móvil	La existencia de credenciales por defecto y/o la aceptación o uso de contraseñas débiles. El almacenamiento inseguro de los datos. La ausente o el inadecuado cifrado de lo que se transporta. Un mecanismo inseguro de recuperación de contraseñas y claves. La ausencia de una autenticación de doble factor
Backend API de proveedores	Aceptar como inherente la confianza en las aplicaciones de la nube o móviles. Mecanismos de autenticación débiles. Los controles de acceso inexistentes o débiles. La posibilidad de que tengan éxito los ataques de inyección. La presencia de servicios ocultos y funcionalidades no documentadas.

Superficie de Ataque	Vulnerabilidad
Comunicación del ecosistema	La ausencia o el abuso de los controles sobre el estado de salud de todo el sistema. Las pruebas de funcionamiento correcto (Heartbeats) del sistema. La (in)seguridad de los comandos que operan el ecosistema. El desaprovechamiento de recursos o capacidades. El forzado de las actualizaciones.
Tráfico de red	La propia Red de Área Local (LAN). El salto desde la LAN a Internet (enrutador, proxy, cortafuegos, etc.). Las conexiones aéreas de corto alcance. La no estandarización de protocolos y/o procedimientos. Las redes inalámbricas en si (Wi-Fi, Z-wave, Zigbee, Bluetooth).
Autenticación y Autorización	La posibilidad de analizar los dispositivos con técnicas de Protocol fuzzing ¹⁹ . La divulgación de valores relacionados con la Autenticación/Autorización de claves de sesión, token, cookies, etc. La reutilización de claves de sesión, tokens, etc. La ausencia de autenticación de dispositivo con dispositivo. La nula o débil autenticación del dispositivo con la aplicación y entre el dispositivo y la nube, y viceversa. La no autenticación de la aplicación con la nube, y viceversa. La falta de autenticación de las aplicaciones Web con el sistema en la nube. La falta de técnicas de autenticación dinámica.
Privacidad	La divulgación de datos de usuario. La publicación de la ubicación del usuario a través del seguimiento de su dispositivo. La posibilidad de sistemas con privacidad diferencial, en la que unos pocos monitorizan a todos y nadie les monitoriza a ellos.



Internet of Things (IoT)

- **Decálogo de seguridad para arquitecturas IoT (Informe de buenas prácticas de IoT - CCN-CERT)**
 - I. Evitar utilizar dispositivos IoT siempre que no sean estrictamente necesarios.
 - II. No utilizar, en la medida de lo posible, aquellos dispositivos IoT que transmiten información a servidores externos (la Nube), incluso si son los del fabricante.
 - III. Cambiar las contraseñas por defecto de los dispositivos y utilizar contraseñas realmente robustas, que no estén en ningún diccionario, que sean suficientemente largas y por tanto difíciles de adivinar.
 - IV. Mantener actualizados los dispositivos con las últimas versiones disponibles de software y firmware.
 - V. Desactivar toda conectividad remota (con Internet) de los dispositivos cuando no sea estrictamente necesaria.
 - VI. Mantener abiertos solo aquellos puertos de comunicación que sean realmente necesarios y modificar los puertos de escucha si es posible.
 - VII. Si los dispositivos IoT no permiten la configuración de su seguridad, operar con ellos siempre en una red de área local (LAN) detrás de un dispositivo (enrutador) correctamente configurado que sí provea esa seguridad.
 - VIII. En la medida de lo posible, asegurar la autenticidad, confidencialidad e integridad en todas las comunicaciones locales (LAN), especialmente si estas se realizan por enlaces radio (Wi-Fi, Bluetooth, etc.).
 - IX. Comprobar periódicamente y sin previo aviso, la configuración de seguridad de todos los elementos de la arquitectura IoT y de sus dispositivos de comunicación con el exterior.
 - X. Comprobar la visibilidad de los dispositivos propios en buscadores de dispositivos IoT como Shodan.

Internet of Things (IoT)



Tabla de contenidos

- **Conceptos**
- **Seguridad de la Información**
- **IoT: Internet of Things**

Introducción

