Incidentes de Ciberseguridad

Curso de Especialización de Ciberseguridad en las Tecnologías de la Información

Juan Gualberto Guitérrez Marín

Copyright © 2022 Juan Gualberto Gutiérrez Marín

PUBLISHED BY D. INFORMÁTICA - IES VIRGEN DEL CARMEN

HTTP://JUANGUALBERTO.GITHUB.IO.

Licensed under the Creative Commons Attribution-NonCommercial 3.0 Unported License (the "License"). You may not use this file except in compliance with the License. You may obtain a copy of the License at `http://creativecommons.org/licenses/by-nc/3.0`. Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

Primera Edición, Enero 2022

Índice general

I **Primera Parte**

1 **A quién va dirigido este libro** 11

2 **Introducción a la Ciberseguridad** 13

2.1 Seguridad Física y Lógica **14**

2.2 Dimensiones de la seguridad **14**

2.3 Ciberseguridad **15**

2.4 Ciberresiliscencia **15**

2.5 Vulnerabilidades **16**

2.5.1 Herramientas/utilidades para detectar vulnerabilidades 17

2.5.2 Incidentes de ciberseguridad 18

2.5.3 MITRE ATT&CK 18

2.5.4 El INCIBE 19

2.5.5 Tipologías de incidentes de seguridad 19

2.5.6 El proceso de gestión de incidentes 20

2.5.7 Normas o metodologías de gestión de incidentes 20

2.6 Herramientas/software para gestión incidentes **25**

2.7 Criptografía **27**

2.7.1 Algoritmos de Hash 27

2.8 La importancia de la concienciación **28**

2.8.1 Ingeniería Social 29

2.9 Malwares **32**

2.9.1 Adware 32

2.9.2 Gusano . . . 33
2.9.3 Keylogger . . . 33
2.9.4 Ransomware . . . 33
2.9.5 Rogue Software . . . 33
2.9.6 Rootkit . . . 33
2.9.7 Spyware . . . 34
2.9.8 Virus . . . 34
2.9.9 Externalización de la ciberseguridad . . . 34

II Segunda Parte

3 Normativa. Políticas y Auditorías . . . 37
3.1 El sistema de gestión de incidentes 37
3.2 Plan Director de Seguridad 37
3.2.1 Preparación . . . 38
3.2.2 Identificación . . . 38
3.2.3 Contención . . . 39
3.2.4 Erradicación . . . 39
3.2.5 Recuperación . . . 40
3.2.6 Recapitulación . . . 40
3.3 Marcos de referencia en gestión de la ciberseguridad 40
3.3.1 El CTN 320 . . . 40
3.3.2 La serie ISO/IEC 27000 . . . 43
3.3.3 ISO 22301 . . . 44
3.3.4 NIST . . . 45
3.3.5 ITIL . . . 45
3.4 Normativa de referencia 46
3.4.1 Normativa nacional . . . 46
3.4.2 Normativa Europea . . . 46
3.5 Requisitos legales (compliance) 48
3.5.1 LOPDGDD . . . 48
3.5.2 RGPD . . . 48
3.5.3 Acceso electrónico de los ciudadanos a los Servicios Públicos . . . 48
3.5.4 ENS . . . 49
3.5.5 PIC . . . 49
3.5.6 PSD2 . . . 50
3.5.7 HIPAA . . . 51
3.6 Auditorías 51
3.6.1 Procedimientos . . . 52
3.6.2 Herramientas de auditoría . . . 52
3.7 Certificaciones Oficiales 52
3.7.1 ISACA . . . 52
3.7.2 (ISC)² . . . 53
3.7.3 EC-Council . . . 53
3.7.4 SANS GIAC . . . 53
3.7.5 CompTIA . . . 53

3.7.6 Offensive Security . . . 53
3.7.7 Cisco Systems . . . 53

4 Plan de prevención y concienciación. . . . 55
4.0.1 Kit de concienciación del INCIBE . . . 56
4.1 Prevención 56
4.1.1 Protección y destrucción de datos . . . 56
4.1.2 Phishing . . . 56
4.1.3 Protección del correo electrónico . . . 56
4.1.4 Enlaces peligrosos . . . 56
4.1.5 Adjuntos peligrosos . . . 56
4.1.6 Ingeniería social . . . 56
4.1.7 Amenazas en la rutina diaria . . . 56
4.2 Compliance (cumplimiento normativo) 56
4.2.1 Reglamento General de Protección de Datos (GDPR) . . . 56
4.2.2 PCI DSS Información sanitaria protegida . . . 56
4.2.3 Protección contra el ransomware . . . 56

5 Taxonomía de los incidentes de ciberseguridad . . . 57
5.1 Contenido Abusivo 60
5.2 Código Malicioso 61
5.3 Recolección de información 61
5.4 Intento de intrusiones 62
5.5 Intrusiones 62
5.6 Disponibilidad 62
5.7 Seguridad y confidencialidad de la información 63
5.8 Fraude 63
5.9 Vulnerabilidades 63
5.10 Otros 63
5.11 Bibliografía para ampliar 63

III Tercera Parte

6 OSINT . . . 67
6.1 Recopilación de datos 68
6.2 Metodología 70
6.2.1 Modos de recopilación de información . . . 71
6.2.2 El entorno de trabajo . . . 71
6.3 Casos prácticos 72
6.3.1 Modelo de actuación para casos de phising . . . 72

6.4 LinuxMint OSINT 72
6.4.1 Herramientas para Youtube . . . 73
6.4.2 Herramientas para Instagram . . . 73
6.4.3 Herramientas de usuario / correo electrónico . . . 74
6.4.4 Herramientas para analizar redes (CLI) . . . 74
6.4.5 Herramientas para investigar redes (Web) . . . 74
6.4.6 Herramientas de Telegram . . . 76
6.4.7 Herramientas de Office 365 . . . 76
6.4.8 Herramientas búsqueda de código . . . 76
6.4.9 Herramientas para investigar Proton Mail y VPN . . . 76
6.5 Herramientas on-line 76
6.5.1 Webs para buscar archivos en servidores FTP . . . 76
6.5.2 Webs para ampliar conocimientos sobre OSINT . . . 76

IV Cuarta Parte

7 Preparación. Configuraciones seguras. MITRE . . . 79
7.1 ¿Y si sucede un incidente? 80
7.1.1 Comunicación del incidente . . . 81
7.1.2 Sistema de ventanilla única . . . 81
7.1.3 Criterios para la notificación . . . 82
7.2 Mecanismos de defensa 85
7.2.1 Introducción al SOC . . . 85
7.2.2 IDS Snort . . . 89
7.2.3 Bastionado de redes: Network Security Monitoring (NSM) . . . 89
7.2.4 Security Onion . . . 89
7.2.5 Zeek (Bro) . . . 91
7.2.6 IDS Avanzado . . . 91
7.2.7 NOC con pfSense . . . 91
7.2.8 Servicios de VPN . . . 91
7.2.9 Snort como IPS en pfSense . . . 91
7.2.10 NETFLOW . . . 91
7.3 Mitre ATT&CK 91

8 Detección de incidentes . . . 93
8.1 IDS 93
8.2 SOC 93
8.3 SIEM 93

9 Respuesta ante incidentes . . . 95
9.1 Contención 95
9.2 Erradicación 95
9.3 Recuperación 95

10 Actividad postincidente 97
10.1 Documentación, evidencias y ciclo de mejora 97

V Quinta Parte

11 Inteligencia artificial 101
11.1 Inteligencia artificial aplicada a la ciberresiliscencia 101

VI Bibliografía, webs y programas recomendados

Bibliography 105
Articles 105
Books 105
Books 105
Books 105

Primera Parte

1 A quién va dirigido este libro 11

2 Introducción a la Ciberseguridad 13

2.1 Seguridad Física y Lógica
2.2 Dimensiones de la seguridad
2.3 Ciberseguridad
2.4 Ciberresiliscencia
2.5 Vulnerabilidades
2.6 Herramientas/software para gestión incidentes
2.7 Criptografía
2.8 La importancia de la concienciación
2.9 Malwares

1. A quién va dirigido este libro

Este libro está principalmente orientado a técnicos del sector de las TIC interesados en el apasionante mundo de la ciberseguridad, especialmente aquellos del lado de la empresa interesados en proteger la integridad, veracidad y acceso a los datos de la misma.

¿Son necesarios conocimientos previos?. Aunque haremos una breve introducción de todas las tecnologías y/o lenguajes de programación que el lector pueda necesitar, a grandes rasgos necesitarás:

- Moverte *como pez en el agua* con la terminal tanto en sistemas Unix (Linux/Mac/etc.) como Windows.
- Leguajes de programación como Python, así como nociones de Bash y PowerShell scripting.
- Conocimentos de redes como: direcciones IPv4, IPv6, máscara de red, VLAN, tecnologías WiFi (como 802.11 a,b,n WPA 1,2,3).

2. Introducción a la Ciberseguridad

"El arte de la guerra se basa en el engaño. Por lo tanto, cuando es capaz de atacar, ha de aparentar incapacidad; cuando las tropas se mueven, aparentar inactividad."

El Arte de la Guerra (Sun Tzu).

En julio de 2017 un grupo de hackers utilizaron una pecera "inteligente" para entrar en los sistemas de información de un casino de Las Vegas. Se trataba de una pecera que estaba remotamente monitoreada, ajusta la temperatura automáticamente, así como la salinidad y alimentación de los peces (fuente: `https://www.forbes.com/sites/leemathews/2017/07/27/criminals-hacked-a-fish-tank-to-steal-data-from-a-casino`).

El inusual tráfico de red levantó la sospecha de que algo extraño estaba ocurriendo. Para cuando la empresa de ciberseguridad se hizo cargo, los ciberdelincuentes ya se habían llevado más de 10 GB de datos.

Este ejemplo pone de manifiesto cómo de frágil es la tecnología si no es tratada por expertos. Hoy en día oímos hablar de la Industria 4.0, de cómo las tecnologías habilitadoras digitales (THD) van a facilitar la revolución tecnológica...

Si no ha oído hablar de las THD, algunos ejemplos son:

- Cloud Computing
- Internet de las Cosas (IoT)
- Big Data
- Realidad aumentada y virtual
- Modelado/impresión 3D
- Inteligencia Artificial
- Machine Learning
- Blockchain
- 5G

Empresas y particulares, deslumbrados por estas tecnologías emergentes, algunas hasta disrruptivas, adoptan tecnologías que aún no dominan plenamente, creando un caldo de cultivo idóneo para los ciberdelincuentes: la tormenta perfecta...

Hasta hace unos años bastaba con atrincherarse tras poderosos cortafuegos en nuestra inexpugnable LAN, pero desde que apareció "la nube", la mayor parte de nuestros datos, y los de nuestras empresas, no están en el cuarto de servidores, ni siquiera en nuestra ciudad sino que, probablemente, estén distribuidos en *datacenters* a lo largo del planeta. Nuestro código fuente quizás está en Gitlab, nuestro software corre en AWS, la información de nuestros sistemas en DynamoDB…

Y aún no hemos hablado de la presencia tanto de nuestra empresa como nuestros trabajadores en redes sociales, quizás usando infraestructuras de la empresa, como WiFi o redes cableadas para conectar a ellas, o instalando programas en equipos de la empresa para usarlas ¿puede ser eso otro peligro?

Un atacante puede estar motivado por muchos factores, como equipo de respuesta, raramente conoceremos desde el inicio la verdadera motivación y muchas veces ni si quiera llegaremos a conocerla. Atribuir un ataque a un grupo de hackers, colectivo o país es una ardua tarea, a veces imposible. La **inteligencia contra amenazas** nos provee de pistas vitales para catalogar tácticas, técnicas, procedimientos y herramientas de estos grupos, conocer sus contrainteligencias, desinformación, y falsos positivos que nos pueden hacer mirar en la dirección opuesta del verdadero riesgo.

"Los malos" nunca descansan. Gracias a Internet aquí pueden ser las 4:00 am pero allí las 5:00 pm, además saben que los fines de semana estamos menos personal atento, conocen mejor que nosotros nuestras debilidades... El equipo de respuesta a ciberamenazas debe estar disponible 24/7 los 365 días del año. Es por ello que, como veremos más adelante, podemos implementarlo nosotros, externalizarlo parcialmente o totalmente.

Cada día se están librando cientos de guerras y el campo de batalla ahora es el ciberespacio.

Este texto pretende ser, primero una concienciación a los peligros que nos aguardan en el mundo digital, y segundo una base para estar preparados para ellos. Un manual para quien quiera iniciarse en el "blue team".

Comencemos repasando algunos conceptos básicos.

2.1 Seguridad Física y Lógica

Llamamos seguridad física a la que protege el accesos no autorizados o ataques físicos a nuestros equipos. Por ejemplo, los servidores o armarios de datos de la organización "X Corp" están custodiados es una habitación guardada bajo llave y con sistemas especiales de refrigeración y extinción de incendios.

Llamamos seguridad lógica a la que protege la información en uso, a como archivos, almacenes de datos, información en memoria RAM o programas de gestión. Ejemplos:

- En una organización disponen de usuarios para acceder a sus sistemas y listas de control de acceso (ACL) para tener control de los privilegios (programas, archivos, datos) que pueden ver y usar.
- Hay una política de copias de seguridad para poder restablecer el servicio en caso de contingencias.

2.2 Dimensiones de la seguridad

Típicamente los pilares o dimensiones básicas de la seguridad son tres: confidencialidad, integridad y disponibilidad. Deben de existir al menos estos tres pilares para poder hablar de seguridad.

No obstante, en toda empresa de la sociedad de la información, encontraremos estas cinco dimensiones (preceptivas) de la seguridad:

- **Disponibilidad**: la capacidad de un servicio, un sistema o una información, a ser accesible y utilizable por los usuarios o procesos autorizados cuando éstos lo requieran. Actúa sobre la no interrupción del servicio.
- **Confidencialidad**: propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. Previene la filtración de información.
- **Integridad**: garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción, ya sea de forma accidental o intencionada, por errores de software o hardware o por condiciones medioambientales. previene manipulaciones de la información. La integridad está formada también por la autenticidad y el no repudio (ej: el no repudio prueba que el emisor envió la comunicación -no repudio en origen- y que el destinatario la recibe – no repudio en destino-).
- **Autenticidad**: una entidad es quien dice ser o bien se garantiza la fuente de la que proceden los datos. Protege el aseguramiento de la identidad.
- **Trazabilidad**: permite conocer posibles rastros en accesos.

2.3 Ciberseguridad

La ciberseguridad da un paso más y añade a la seguridad lógica protección contra ataques, de tal manera que podemos definirla como la inteligencia (conocimiento), medios y técnicas que usamos para proteger de ataques maliciosos.

El objetivo de la ciberseguridad es desarrollar acciones y normas que minimicen el riesgo o, en el peor caso, el impacto de un posible ataque contra las infraestructuras, información o usuarios de nuestra organización. Pero ¿cómo hacerlo?, con buenas prácticas como por ejemplo:

- Teniendo siempre actualizados todo el software a las últimas versiones
- Usando sistemas de detección de malware en los equipos e intrusiones en nuestras redes
- Controlando los accesos a los sistemas
- Gestionando las altas y bajas del usuarios (si un usuario no trabaja aquí ya, no puede estar en los sistemas su usuario operativo)
- Teniendo una buena política de contraseñas
- Realizando copias de seguridad periódicas
- Analizando, gestionando y reportando los **incidentes de seguridad** (en inglés DFIR – Digital Forensics and Incident Report)
- Planificando la recuperación ante desastres para reducir el tiempo para volver a estar operativos

Sin embargo sólo con buenas prácticas no alcanzaremos un buen nivel de seguridad, no sin aplicar normas o estándares que nos ayuden en el proceso de securizar nuestros sistemas de información.

2.4 Ciberresiliscencia

En 2019, el U.S. National Institute of Standards and Technology (NIST) liberó la publicación especial 800-160 volumen 2 titulado “Desarrollando Sistemas Ciberresiliscentes: Una aproximación desde la Ingeniería de Seguridad de Sistemas” (`https://doi.org/10.6028/NIST.SP.800-160v2`). Esta publicación se basa en la premisa que prevenir absolutamente todos los ciberataques es imposible y que eventualmente el adversario entrará en nuestras redes.

Partiendo de esta afirmación, se crea el concepto de ciberresiliscencia, que consiste en en la habilidad de anticiparse, resistir y recuperarse de condiciones adversas, estrés, ataques o sistemas comprometidos que incluyen recursos cibernéticos.

2.5 Vulnerabilidades

Antes de introducir el concepto de incidente en sistemas de información, es necesario definir qué es vulnerabilidad. Haciendo un poco de investigación en Internet, encontramos definiciones de vulnerabilidad tan serias como:

- Según el NIST: Debilidad del sistema de información, procedimientos de seguridad del sistema, controles internos o implementación que podrían ser explotados o desencadenados por una fuente de amenaza.
- Según la norma ISO 27005: Una debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas cibernética, donde un activo es cualquier elemento de valor para la organización, sus operaciones comerciales y su continuidad, incluidos recursos de información que apoyan a la misión de la organización.
- Según el IETF RFC 4949: Un defecto o debilidad en el diseño, la implementación o el funcionamiento y la gestión de un sistema que podría ser explotada para violar la política de seguridad del sistema.
- Según ENISA: La existencia de una debilidad, un error de diseño o de implementación que puede conducir a un evento inesperado e indeseable que comprometer la seguridad del sistema informático, la red, la aplicación o el protocolo en cuestión.
- The Open Group: La probabilidad de que la capacidad de la amenaza exceda la capacidad de resistir a la misma.
- Factor Analysis of Information Risk: La probabilidad de que un activo sea incapaz de resistir las acciones de un agente que la amenaza.
- ISACA: Una debilidad en el diseño, la implementación, el funcionamiento o el control interno.

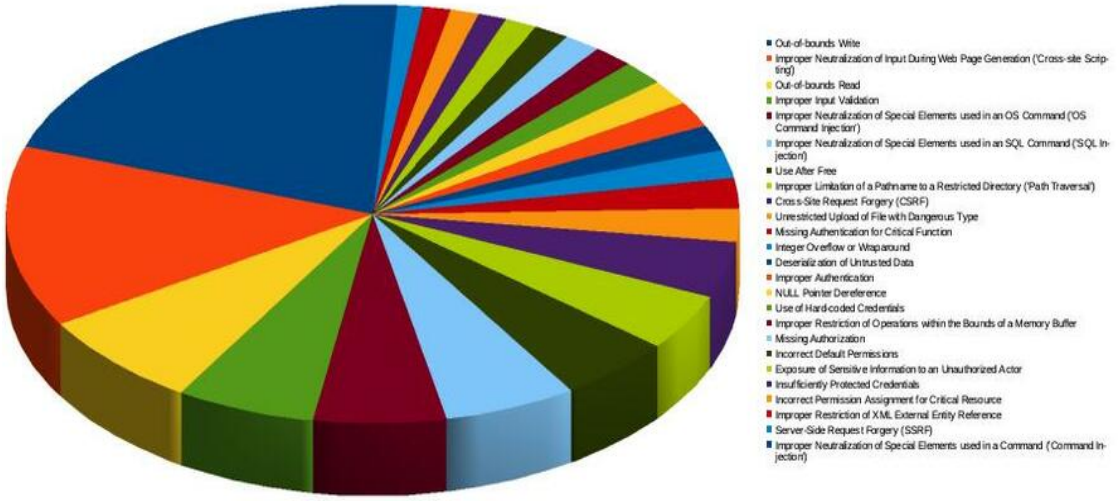
Nosotros, identificaremos una vulnerabilidad como un fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma. Las vulnerabilidades de este modo suponen amenazas, que potencialmente pueden ser explotadas por atacantes que quieran sacar provecho de las mismas, según un riesgo o probabilidad de que se produzca un incidente de seguridad.

Las vulnerabilidades se deben principalmente a fallos en la programación de los sistemas de información, es decir errores que los programadores cometen con regularidad. De hecho, existen diferentes entidades que recopilan e informan de los errores más comunes para que podamos preverlos y evitarlos. Existen incluso bases de datos en abierto, libres para consulta, de vulnerabilidades.

Entre las Web más conocidas están:

- CWE (Common Weakness Enumeration): Listado de errores más comunes de MITRE. `https://cwe.mitre.org/index.html`
- OWASP Top 10: Listado de los errores más comunes en aplicaciones Web. `https://owasp.org/www-project-top-ten/`

Imagen 1: 2021 CWE Top 25 Most Dangerous Software Weaknesses. https://cwe.mitre.org/top25/archive/2021/2021_cwe_top25.html



2.5.1 Herramientas/utilidades para detectar vulnerabilidades

Probablemente si es programador y haya leído en el apartado anterior que existen bases de datos de vulnerabilidades, se haya encendido esa lucecita con la pregunta ¿hay entonces programas para automatizar la tarea de escaneo de mi software en busca de vulnerabilidades?

La respuesta, por supuesto es que sí, de hecho existen en el mercado multitud de herramientas como por ejemplo:

- **Nessus**: Uno de los más veteranos (desde finales de los 90' en el mercado). Inicialmente GPL pero de pago en las versiones más actuales. Multiplataforma.
- **OpenVAS**: ahora Open Vulnerability Assessment Scanner. Es el fork gratuito de Nessus. Se trata del escáner del sistema integral de gestión de vulnerabilidades GVM (Greenbone Vulnerability Manager).
- **NeXpose**: solución de pago para analizar las vulnerabilidades, los controles y las configuraciones, y encontrar el quién, el qué, y el dónde de los riesgos de TI de seguridad.
- **FaasT** (Web): Servicio de persistent pentesting que detecta las debilidades y vulnerabilidades de una organización antes que los atacantes.
- **SAINT:** Una de las funciones de esta herramienta es el escaneo de vulnerabilidades, está basado en la conocida SATAN. Al igual que ocurre con Nessus, hay una parte de pago y otra libre.

Herramientas de descubrimiento como Nmap/Zenmap, MASSCAN, Fing, etc. no son realmente escáneres de vulnerabilidades, aunque sí pueden ayudar, y mucho, en la preparación del listado de activos de la red de la empresa.

Ciclo de gestión de vulnerabilidades

Obviamente, no basta con disponer de una buena herramienta para el análisis de vulnerabilidades, también es necesario completar un proceso o ciclo de gestión de vulnerabilidades. Este ciclo

debe comprender, al menos, los siguientes pasos:

1. **Inventario de activos**: listado de todos los dispositivos hardware, software instalado y versiones de los mismos, software de propio desarrollo...
2. **Detección de vulnerabilidades**: con ayuda de una herramienta de escaneo (realizar esta tarea de manera manual sería tedioso), se prepara un listado activos además de sus vulnerabilidades.
3. **Análisis de amenazas**: se clasifican por tipo o severidad. Se establece un nivel de prioridad en base a la probabilidad de explotación (por ejemplo: crítica, alto, medio y bajo).
4. **Remediación**: cuando sea posible, se "parchean" o actualizan los equipos afectados. No siempre será posible, hay vulnerabilidades que no tienen solución.
5. **Validación**: Comprobamos que el remedio ha funcionado antes de poner el equipo/servicio de vuelta en producción. Si no lo ha hecho, hay que volver al paso 2.
6. **Aplicación**: Si hemos validado correctamente, ya sabemos la solución para este problema en casos futuros.

2.5.2 Incidentes de ciberseguridad

"By Failing to Prepare, You Are Preparing to Fail" – Benjamin Franklin.

(si no estás preparado, estás preparado para caer)

Un incidente de ciberseguridad se define como uno o un conjunto de eventos que ocurren de forma inesperada o no deseada, con alta probabilidad de afectar el normal funcionamiento de una empresa, debido a la pérdida o uso indebido de información.

Se trata pues de cualquier evento no deseado que compromete la confidencialidad, integridad o disponibilidad de la información y que da lugar, o lo intenta e forma explícita, a un perjuicio para la empresa.

Nuestro trabajo es entonces diseñar y ofrecer un buen proceso de gestión de incidentes. Precisamente este libro se centra en dicho proceso y pretende ser tanto una introducción a la ciberseguridad en la empresa como un compendio tanto de buenas prácticas.

Esta gestión no es un problema al que hacer frente desde cero, no estamos solos, sino que disponemos de todo un abanico de organizaciones que nos ofrecen sus servicios y conocimiento en este quehacer. Otras, incluso, nos brindarán soporte y ayuda. A continuación vamos a conocer algunas de ellas.

2.5.3 MITRE ATT&CK

MITRE es una ONG de EEUU que provee ingeniería de sistemas, investigación y desarrollo, y soporte sobre tecnologías de la información.

Las Tácticas, Técnicas y Conocimientos Comunes del Adversario de MITRE (ATT&CK) es una base de conocimiento accesible a nivel mundial de tácticas y técnicas adversas basadas en observaciones del mundo real de las amenazas a la seguridad cibernética. Se muestran en matrices organizadas por etapas de ataque, desde el acceso inicial al sistema hasta el robo de datos o el control de la máquina. Existen matrices para plataformas de escritorio comunes (Linux, macOS y Windows), así como para plataformas móviles.

Veremos más información sobre MITRE y su ATT&CK en capítulos posteriores.

El CCN-CERT

El Centro Criptológico Nacional Computer Emergency Response Team, también conocido por su sigla CCN–CERT, es el organismo español, creado en 2006, encargado de contribuir a la ciberseguridad de la administración pública, los organismos públicos y empresas estratégicas del

país. CCN-CERT depende directamente del Centro Criptológico Nacional, del que toma parte de su nombre.

Hacemos aquí un inciso para explicar este término de CERT. Con la cantidad de ciberataques que ocurren diariamente, muchas empresas y organismos gubernamentales necesitaban desarrollar un equipo de personas especializadas que pudieran responder a estos ataques. Ese es el origen del Equipo de Respuesta a Emergencias Cibernéticas (CERT) o Equipo de Respuesta a Incidentes de Seguridad Cibernética (CSIRT).

2.5.4 El INCIBE

Como podemos ver en su Web, el El Instituto Nacional de Ciberseguridad de España (INCIBE), anteriormente Instituto Nacional de Tecnologías de la Comunicación, es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos.

La compañía se dedica a dar soporte en materia de seguridad informática a ciudadanos, empresas públicas y privadas, así como a las administraciones públicas y sus organismos, y a instituciones académicas y de investigación, especialmente aquellas que gestionan infraestructuras críticas. Asimismo, participa en la Estrategia Nacional de Ciberseguridad.

2.5.5 Tipologías de incidentes de seguridad

Según la ENISA (`https://www.enisa.europa.eu/publications/reference-incident-classificat` podemos hacer una primera clasificación de los incidentes en:

Clasificación	Ejemplo
Contenido abusivo	▪ Spam ▪ Violencia ▪ Pornografía infantil
Código malicioso	▪ Virus ▪ gusano ▪ troyano ▪ spyware ▪ dialer ▪ rootkit
Recolección de información	▪ escaneo de puertos/servicios ▪ sniffing ▪ ingeniería social
Intentos de intrusión	▪ explotación de vulnerabilidades conocidas ▪ intentos de login ▪ exploits 0day

Intrusiones	▪ Cuentas comprometidas ▪ bots
Disponibilidad	▪ DoS ▪ DDoS ▪ sabotajes ▪ errores humanos
Acceso	▪ Accesos no autorizados ▪ Modificaciones no autorizadas
Fraude	▪ Uso no autorizado de recursos ▪ Infringimiento de copyright ▪ Phising
Vulnerabilidad	▪ Impresoras/copiadoras sin contraseña ▪ Antivirus no actualizados ▪ Sistemas no actualizados

2.5.6 El proceso de gestión de incidentes

El proceso de gestión de incidentes define conjuntos de actividades que son realizadas por parte del CERT independientemente de que se esté respondiendo a un incidente o no.

De manera general toda norma o estándar siempre va a contener a estos tres procesos básicos:

- Proceso de planificación y preparación para enfrentar incidentes de seguridad, que comprende:
  - elaboración de políticas de seguridad
  - actualización de las políticas
  - concienciación y entrenamiento
- Proceso de atención/respuesta a incidentes:
  - detección y reporte de eventos
  - evaluación y decisión de acciones necesarias
  - respuesta ante el incidente
- Proceso de mejora continua para enfrentar futuros incidentes
  - mejoras en la postura de seguridad
  - mejoras en el plan de atención de incidentes

2.5.7 Normas o *metodologías* de gestión de incidentes

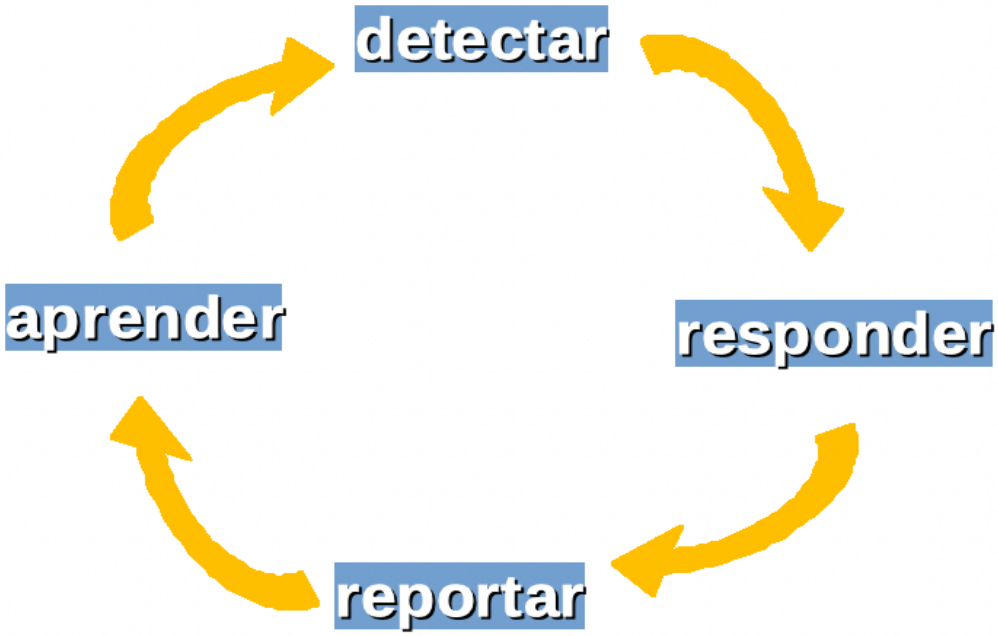
Una buena gestión de incidentes, permite desarrollar correctamente una respuesta ante dichos incidentes. Para llevar a cabo dicha gestión, nos apoyamos en metodologías, que suelen ser normas o estándares bien conocidos.

Sin un control exhaustivo de los registros de todos nuestros sistemas, buenos diagramas de red, inventario de todos los activos (hardware y software), en general una buena organización, no podemos aplicar ninguna metodología. Antes de empezar a trabajar este punto es imprescindible tener organizada y detallada toda esta información.

La gran mayoría de metodologías usan el ciclo PICERL:

1. Preparación: Establecimiento de políticas, procedimientos, formación...
2. Identificación: Procesos, eventos o tráfico de red inusual...
3. Contención: Priorizar, categorizar, recolección de evidencias...
4. Erradicación: Actualización, parcheo...
5. Recuperación: Volver a estar operativos...
6. Lecciones aprendidas: Documentar, actualizar procedimientos, actualizar políticas...

Figura 1: SANS 504B Incident Response Cycle CheatSheet.https://www.sans.org/media/score/504-incident-response-cycle.pdf



ISO 27035:2016

La Organización Internacional de Normalización (ISO) de estándares, dispone la norma 27035 para la Gestión de Incidentes de Seguridad de la Información

Partiendo de un ciclo de mejora continua, posteriormente plantea un ciclo de cinco fases para la gestión de incidentes. Según esta norma, los pasos para gestionar correctamente un incidente de seguridad deberían ser al menos:

1. **Notificación del incidente**: nuestros IDS (sistemas de detección de intrusiones), personal técnico, usuarios... detectan un evento que puede dañar el funcionamiento de la organización, por lo que se comunica el incidente de acuerdo con los procedimientos de la organización (por lo general una plataforma de gestión de incidencias o tickets o bien correo electrónico)
2. **Clasificación del incidente**: el personal que recibe la notificación del incidente lo clasifica. El IDS o la persona que detecta el incidente también puede hacer una clasificación, pero es un experto técnico quien debe concretarlo adecuadamente.
3. **Tratamiento del incidente**: una vez clasificado y se determina la gravedad y el tiempo acordado para su resolución, un técnico debe decidir sobre las medidas necesarias para resolverlo.
4. **Cierre el incidente**: cuando se resuelve el incidente, se registra toda la información generada durante el tratamiento y, si es necesario, se notifica a la persona que envió primero la

notificación del incidente que se cerró.

5. **Base de conocimiento**: toda la información generada durante el tratamiento del incidente es crítica para posibles incidentes similares en el futuro, así como para recopilar evidencias. La información generada para resolver el incidente se registra, por si el problema vuelve a ocurrir en el futuro, llegar rápidamente a la solución perfecta sin perder tiempo.

NIST SP 800-61 R2

Por supuesto que la ISO 27035 no es el único estándar de gestión de incidentes. La guía 61 de la serie SP800 del NIST: "Computer Security Incident Handling Guide" (`https://doi.org/10.6028/NIST.SP.800-61r2`), propone otro estándar para ello. En este caso el proceso varía ligeramente, siguiendo este esquema:

Figure 2: El proceso de gestión de incidentes

Como podemos ver comenzamos con un proceso de prevención, que incluirá la formación y concienciación de los empleados así como la implicación de la directiva de la empresa.

Seguiremos con medidas de detección y análisis (por ejemplo: un antivirus, un sistema de detección de intrusiones o IDS).

A continuación entramos en la fase de contención, erradicación y respuesta, aquí entran ya factores humanos (nosotros somos los encargados de hacerlo) o incluso sistemas inteligentes. Por ejemplo, un EDR o ETDR, Endpoint Thread Detection and Response es capaz, a partir de actividad inusual en nuestra red, analizar esos patrones sospechosos y responder o contener dicha actividad. Otro ejemplo podría ser la protección antiransomware disponible a partir de Windows 10.

Es importante darse cuenta que, una vez un sistema ha sido comprometido, no podemos darlo por confiable hasta volver a hacerle más pruebas de detección y análisis (una cuarentena).

De las batallas (ganadas y perdidas) hay que hacer introspección, analizar nuestra situación actual y hacer propuestas de mejora.

Conclusiones

Aunque es altamente recomendable seguir un estándar de seguridad, es muy importante destacar que ***la ciberseguridad debe ser parte de la estrategia de la empresa***, para ello muchos expertos coinciden en estas **cinco claves para la estrategia de ciberseguridad**:

- Anticipación y prevención: Hay que tener un ***plan*** de respuesta.
- ***Detección*** y análisis con una seguridad inteligente: Los antivirus tradicionales dan paso a los EDR o End Point Detection and Response (sistemas inteligentes capaces de detectar amenazas o ataques a nuestros servidores Web, por ejemplo)
- ***Triaje*** y análisis: Para poner dar la mejor respuesta al incidente y estar prevenidos para futuros incidentes similares es necesario llevar a cabo un análisis. El análisis que se realiza en este paso debe incluir: análisis binario, análisis del endpoint e idealmente, un servicio Threat Hunting que ofrezca una capa adicional de análisis e investigación.
- ***Contención, erradicación y recuperación***. Una vez detectado el incidente y analizada la causa, es momento de contenerlo. Se debe crear una copia de seguridad de todos los dispositivos, sistemas o redes comprometidas por si fuera de utilidad para futuros análisis forenses.
- El postincidente y el "***Zero Trust***". Con lo aprendido de este incidente, puede ser necesariohacer cambios a la estrategia de ciberseguridad para evitar que vuelva a ocurrir. También es necesario actualizar el plan de respuesta a incidentes para reflejar los nuevos procedimientos.

Para que nuestra estrategia de ciberseguridad sea eficaz debemos realizarla en base a las siguientes premisas:

- Debemos ser proactivos para prevenir mejor los incidentes, para ello tenemos que:
  - Valorar efectos económicos y de reputación de la compañía
  - Adecuar los esfuerzos dedicados a la ciberseguridad a las necesidades de la empresa
  - Inculcar la cultura de la seguridad
- Hay que crear sinergias, alianzas con otras empresas.
  - La unión hace la fuerza
  - Proteger los datos de clientes y exigir a proveedores estar a la altura
  - Cumplir con la normativa de referencia
  - Hacer frente común ante ciberdelincuentes
- Mejora continua.
  - La tecnología está en continuo cambio
  - Hay que renovar las políticas de seguridad, formar al personal y revisar estrategias con frecuencia

Es fundamental dejar claro que nuestros sistemas y procedimientos de respuesta deben actualizarse continuamente. Además es importante recalcar la importancia de hacer frente común a los ciberdelincuentes junto con nuestros proveedores, clientes, entidades gubernamentales...

Figure 3: Relaciones con partes interesadas.

Si conoces algunas normas del catálogo ISO (como la ISO 9001:2015) verás que hay muchas similitudes con esto último y también con el concepto de partes interesadas. Partes interesadas son mis clientes, mis proveedores, las agencias gubernamentales con las que me relaciono, es por eso que el equipo de respuesta de ciberincidentes debe de estar en comunicación con todos ellos.

TLP

En el capítulo anterior hemos hablado de compartir información con nuestros equipos de respuesta, nuestros clientes, proveedores, agencias gubernamentales, pero ¿esa información se hará pública? ¿puede o va a tener impacto en la imagen de nuestra empresa o la confianza de nuestra marca?

Para ello en el sector hay un modo de indicar cómo tratar esta información a los receptores de nuestros mensajes, el TLP.

Traffic Light Protocol (TLP) es un esquema creado para fomentar un mejor intercambio de información sensible (pero no clasificada) en el ámbito de la seguridad de la información.

Fue creado originalmente a principios del decenio de 2000 por el Centro Nacional de Coordinación de Seguridad de la Infraestructura del Gobierno del Reino Unido para promover un mayor intercambio de información sensible. Aunque no fue diseñado originalmente para la ciberseguridad, nuestra industria ha adoptado ampliamente este enfoque para compartir información sensible relacionada con los ataques cibernéticos y la documentación interna

Se utiliza un código de cuatro colores, cuyo significado se puede consultar en la siguiente tabla:

CODIGO	Cuándo usarlo	Cómo compartir	Color	Fondo
TLP:RED	Se debe utilizar TLP:RED cuando la información está limitada a personas concretas, y podría tener impacto en la privacidad, reputación u operaciones si es mal utilizada.	Los receptores no deben compartir información designada como TLP:RED con ningún tercero fuera del ámbito donde fue expuesta originalmente.	#ff0033	#000000
TLP:AMBER	Se debe utilizar TLP:AMBER cuando la información requiere ser distribuida de forma limitada, pero supone un riesgo para la privacidad, reputación u operaciones si es compartida fuera de la organización.	Los receptores pueden compartir información indicada como TLP:AMBER únicamente con miembros de su propia organización que necesitan conocerla, y con clientes, proveedores o asociados que necesitan conocerla para protegerse a sí mismos o evitar daños. El emisor puede especificar restricciones adicionales para compartir esta información.	#ffc000	#000000
TLP:GREEN	Se debe utilizar TLP:GREEN cuando la información es útil para todas las organizaciones que participan, así como con terceros de la comunidad o el sector.	Los receptores pueden compartir la información indicada como TLP:GREEN con organizaciones afiliadas o miembros del mismo sector, pero nunca a través de canales públicos.	#33ff00	#000000
TLP:WHITE	Se debe utilizar TLP:WHITE cuando la información no supone ningún riesgo de mal uso, dentro de las reglas y procedimientos establecidos para su difusión pública.	La información TLP:WHITE puede ser distribuida sin restricciones, sujeta a controles de Copyright.	#ffffff	#000000

2.6 Herramientas/software para gestión incidentes

Para defender de una manera efectiva los activos de nuestra compañía, necesitaremos un buen sistema de detección de incidentes, triaje, contención y respuesta. A continuación vamos a ver un listado de herramientas de las que hablaremos más detenidamente en capítulos posteriores.

- Husmeadores de red (sniffers)
  - tcpdump (disponible en cualquier sistema *NIX). Herramienta de muy bajo nivel, modo texto, para la CLI.
  - Windump (la versión “amigable” de la anterior para sistemas Windows)
  - netcat (la gran alternativa a tcpdump)
  - IPTraf (para sistemas *NIX), herramienta para la consola que permite estadísticas de tráfico, filtrar por host, pero con una interfaz básica.
  - Microsoft Message Analyzer (para Windows 10)
  - WireShark (si no te suena, aún debes formarte más antes de comenzar con este libro)
  - EtherApe (exclusivo para sistemas *NIX)
  - Capsa Network Analyzer (dispone de versiones de pago y gratuitas)
  - Kismet (centrado en redes wireless)
  - NetworkMiner (relamente es una NFAT - Network Forensic Analysis Tool): Excelente alternativa a WireShark.
- Sistemas de detección/prevención de intrusiones o IDS / IPS:
  - SNORT: Uno de los grandes, desde finales de los 90, open source y gratuito. Permite registrar eventos en bitácoras de texto o bases de datos abiertas. Implementa un motor de detección de ataques y escaneo de puertos que permite registrar, alertar y responder ante cualquier anomalía previamente definida. Dispone de una base de datos en abierto y otra de pago de eventos. Es muy conocido por su gran eficiencia (bajo consumo de recursos para el gran trabajo que realiza).
  - Suricata: Otro de los más concidos IDS e IPS, también open source. Cuando apareció allá por 2010, presentaba una gran ventaja frente a Snort, que era multihilo (de hecho y

en sistemas con más de un núcleo era más eficiente.
    - BroIDS: Otra herramienta open-source para el análisis de tráfico de red. Además de IDS, también es IPS pues podemos asociar acciones a una determinada actividad.
    - OSSEC: Más centrado en la intrusión del host que de la red (realmente es un HIDS – Host-based Intrussion Detection), este software open-source, analiza los registros de sistemas Unix, Windows, etc., detecta rootkits y es capaz de alertar y generar respuestas activas.
- Análisis y gestión de registros: SIEM (Security information and event management).
    - ELK: La pila Elastic es capaz de manejar no sólo información sobre registros de seguridad o hacer correlación de eventos con iteligencia artificial, agregar datos, aprender de esos datos con aprendizaje automático o machine learning, sino que también podría hacerlo de otras materias. Se trata de un sistema más general que nosotros usamos para un propósito específico. Es muy conocida por ofrecer una versión libre. La parte de aprendizaje automático es de pago.
    - Splunk Enterprise Security: Uno de los grandes en el que confían las compañías más grandes de la lista Forbes.
    - SolarWinds Security Event Manager: Probeblemente al lector le suene este nombre, por desgracia, debido a los escándalos de 2020 relacionados con su seguridad, es muy usado en el sector público especialmente de EEUU.
    - ArcSight Security Operations: Están trabajando duro, junto a automatización de ingesta de datos sin apenas configuración de una vasta variedad de productos, es su sistema de análisis de comportamiento y aprendizaje automático.
- NetFlow/sflow: Analizadores de tráfico de red. Si tenemos switches gestionados o inteligentes o routers industriales, probablemente soportarán NetFlow (protocolo de red desarrollado por Cisco para recolectar tráfico de red). Algunas herramientas para gestionar la información generada son:
    - Ntopng y nprobe: disponen tanto de versions de pago como gratuitas.
    - Nfdump: Conjunto de herramientas de código abierto para recolectar y procesar información de sflow y netflow.
    - Nfsen: Interfaz gráfica basada en Web para nfdump.
    - ELK
    - SolarWinds
    - Splunk
- Monitores de tiempo de actividad y disponibilidad: Para ver que nuestros servicios están funcionando correctamente y detectar antes que el cliente si algo falla.
    - Nagios XI
    - SolarWinds
    - Zabbix
- Plataformas gestión incidentes
    - TheHive: Una de las más conocidas y extendidas soluciones de código abierto. https://thehive-project.org
    - NightHawkResponse: Solución de ingesta asíncrona de datos que usa ELK como backend para mostrar los datos de análisis forense. Por desgracia no recibe actualizaciones desde hace tiempo. `https://github.com/biggiesmallsAG/nightHawkResponse`
    - Wazuh: Solución de código abierto basado en la pila ELK también. `https://wazuh.com/product/`
    - AlienVault USM: AlienVault es una empresa española adquirida por ATT&T. Se trata

de un conjunto de herramientas para gestión de la ciberseguridad.

- Palo Alto Networks Cortex XDR (eXtended Detection and Response), potentísima solución que combina todo, IDS, IPS, EDR, análisis forense... `https://www.paloaltonetworks.com/cortex/cortex-xdr`
- FIR (Fast Incident Response): Plataforma de gestión de incidentes de código abierto, escrita mayormente en Python. `https://github.com/certsocietegenerale/FIR`
- RTIR (Request Tracker for Incident Response): Se trata de un sistema de notificación y gestión de tickets de incidencias. No recolecta información per se, simplemente permite la comunicación entre cualquier miembro de la empresa y el equipo de seguridad. `https://bestpractical.com/rtir`

Por supuesto no nos hemos olvidado los proveedores de la nube ofrecen también sus propios sistemas de gestión de incidentes como podrían ser AWS Security Hub, Azure Sentinel o Google Chronicle. Los escáneres de vulnerabilidades también recuerdo al lector que lo vimos en un apartado anterior.

Nos hemos dejado en el tintero herramientas de forense (volcado de memoria, análisis de discos, imágenes de discos, de navegadores...), análisis del registro de Windows, ADS (Alternate Data Streams) de Windows, encriptado, desencriptado, y un largo etcétera, pero ya hablaremos de algunas más adelante.

2.7 Criptografía

Según el diccionario de la RAE, esta palabra se compone de cripto- y -grafía, es decir, se trata del arte de escribir con clave secreta o de un modo enigmático.

Imaginemos que Bob quiere mandar un mensaje a Alice, Bob escribe una carta y se la entrega al cartero que sea entregada a Alice. Pero, ¿y si el cartero abre esa carta, altera el texto de la misma, la vuelve a cerrar y la entrega a Alice sin que sea perceptible la alteración? Apliquemos eso a los millones de mensajes que recorren el ciberespacio en cada segundo del día. ¿Cómo sabemos que algunos de ellos no han sido interceptados y alterados por una persona por el camino? Es lo que, a grosso modo, llamamos un ataque MiM o Man in the Middle.

La solución a este problema es la criptografía, de hecho, no habría una Internet segura como hoy día conocemos. Pensemos, de nuevo en el ejemplo anterior, en cómo proteger una conexión a un host remoto. Para saber si nos han "pinchado" la línea, ésta tendría que estar dentro de un tubo con gas, por ejemplo, y si se pierde presión, entonces sabríamos que la línea no es segura. Sería totalmente impracticable.

2.7.1 Algoritmos de Hash

Un algoritmo de hash (no confundir con algoritmos de suma de integridad o checksum) es una función que se aplica a cualquier tipo de archivo de cualquier longitud y siempre da una solución de la misma longitud, independientemente del tamaño del archivo. Dicha función tiene como propósito principal detectar cambios en una secuencia de datos para proteger la integridad de estos, verificando que no haya discrepancias entre los valores obtenidos. La idea es que se transmita el dato junto con su valor hash, de esta forma el receptor puede calcular dicho valor y compararlo así con el valor recibido.

Entre las características que deben de tener estos algoritmos están el bajo coste de cómputo y la no reflexividad, es decir, sea una cadena de bits de salida, debe resultar prácticamente imposible intentar hallar la cadena de origen. De igual manera debe de ser prácticamente imposible encontrar

el mismo hash para un mensaje alterado.

Ejemplos pueden ser: SHA-256, SHA-384 o MD5 (no seguro).

Entre las aplicaciones más destacadas está el blockchain.

Algoritmos de clave simétrica

La criptografía de clave simétrica es un término utilizado para los algoritmos criptográficos que utilizan la misma clave para el cifrado y el descifrado. Ejemplo: el cifrado AES de los discos duros e implementado nativamente en muchos procesadores (AES-NI) o el WPA2/3 del router WiFi de casa.

Algoritmos de clave asimétrica o pública

En los algoritmos de clave asimétrica se usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella.

Ejemplos:

- Diffie-Hellman
- RSA
- Criptografía de curva elíptica

Firma digital y certificados digitales

Volvamos al ejemplo de Bob y Alice. Bob envía un mensaje a Alice de manera que ella esté completamente convencida que fue Bob quien lo envió y que éste, no ha sido alterado por el camino. La solución es usar un algoritmo de llave asimétrica. Bob firma (cifra el hash del mensaje) con su llave privada el mensaje, luego Alice puede, con la llave pública de Bob, saber si él fue el autor del mensaje. De igual forma Bob puede cifrar con la llave pública de Alice el mensaje, de manera que sólo Alice podría leer el mensaje.

Pero los algoritmos asimétricos son muy costosos en tiempo y recursos, y entonces lo que suele hacerse para cifrar un mensaje o conexión es usar un algoritmo de clave simétrica. El ávido lector ya estará preguntando, ¿y cómo acuerdan Bob y Alice esa clave compartida? Sencillo, Bob envía la clave simétrica de un sólo uso a Alice cifrada con la llave pública de Alice, luego ella y sólo ella podría con su llave privada descifrar la clave simétrica de un sólo uso.

Cuando nos conectamos a un servidor Web seguro vía HTTPS, o a un servidor vía SSH, o a la VPN del trabajo, estamos llevando a cabo una operación similar.

La pregunta del millón es, si no todos los servidores Web del mundo tienen mi clave privada, ¿cómo podemos establecer esa conexión segura? Por las relaciones de confianza. Muchos sistemas operativos e incluso navegadores, traen por defecto certificados raíz de confianza de entidades y empresas. Estos certificados raíz de primer nivel sirven para firmar y dar fe que los certificados que hay en los servidores Web son reales y no nos están haciendo un ataque MiM. Es una relación en cadena. Por ello, para una Web pública hay que comprar un certificado digital (también podemos pedir uno gratuito a Let's Encrypt), pagamos no sólo porque generen nuestro certificado, sino también para que lo firmen y así sea de confianza.

2.8 La importancia de la concienciación

En tiempos de pandemia se puso muy de moda el término BYOD (Bring Your Own Device), traer tus propios dispositivos para no tocar o compartir con otras personas. ¿Comparten en en la empresa estos equipos red con los activos de la empresa? Si el equipo de seguridad no tiene acceso

a ellos, ¿cómo podemos saber que no están infectados de un virus o son vulnerables por no estar actualizados? ¿Cómo sabemos que no contienen un troyano que ha implantado la competencia para robarnos nuestros secretos?

En el lado opuesto también está el que trabajaba desde casa con dispositivos de la empresa. ¿Es ético usar ese equipo para entrar en nuestras redes sociales, comprar por Internet o ver esa última serie que acaba de salir? El equipo podría infectarse si lo uso para leer mi correo personal que no pasa por los filtros del correo de la empresa...

Para ir cerrando frentes es fundamental concienciar a la plantilla del buen uso y buenas prácticas de los activos de la empresa.

2.8.1 Ingeniería Social

"Las mejores vulnerabilidades son las personas" Mr Robot.

Según Kevin Mitnick, ingeniería social es la manipulación casual o calculada para influir en las personas y hacerles hacer algo que no harían ordinariamente, convenciéndoles, además, sin levantar la más mínima sospecha. Por cierto que otras de las técnicas de hacking social que gustaban al afamado hacker (como pueden leerse en su libro "Ghost in the Wires") son "tailgating" (colarte con otros empleados en la empresa por la puerta de servicio haciéndote pasar por uno de ellos) y "dumpster diving" (recolectar en la basura evidencias e información de tu víctima).

Un gran amigo y experto en ciberseguridad la define como el troyano humano.

Si buscamos una definición técnica, la ingeniería social se podría decir que es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, credenciales, infecten activos con malware o abran enlaces a sitios infectados.

Debemos entrenar al personal de la compañía a estar siempre alerta y desconfiar de extraños.

Privacidad e identidad digital

A finales de agosto de 2021, Estados Unidos retira sus tropas de Afganistán, después de dos décadas de presencia militar, al frente a una coalición internacional. Durante este tiempo se ha colaborado con personal del país que han ayudado en las tareas de abastecimiento y traducción para las tropas.

Los medios de comunicación locales, en ese tiempo han informado del papel de los soldados y su ayuda para mantener la paz en el país.

Todas las tropas internacionales han abandonado con gran premura el país, dejando atrás instalaciones e incluso sistemas de información. Muchos de estos sistemas están siendo aprovechados por los talibanes para encontrar a las personas que estaban a favor de la presencia militar. Por ejemplo sistema de reconocimiento facial o sistema de reconocimiento de huellas dactilares han sido abandonados en el país. Los talibanes están usando estos aparatos para reconocer a las personas que trabajaban en las bases militares.

De igual forma los noticiarios y las redes sociales reflejan claramente todos estos años de actividad y colaboración entre las tropas extranjeras y los locales. Esta es otra fuente de información para localizar a personas que puedan estar en contra del régimen talibán. Es lo que se conoce como identidad digital (los datos públicos que hay sobre nosotros en el ciberespacio).

Aunque pueda parecer un poco radical, este ejemplo pone de manifiesto como nuestros datos están almacenados por terceros de una manera que no podemos controlar.

Es importante crear una buena conciencia digital sobre la privacidad y sobre nuestros hábitos de Internet, pues puede afectar también a nuestra empresa.

Protección de dispositivos

Imaginemos que nos llevamos a casa un portátil del trabajo para continuar allí la jornada. Paramos un momento para comprar el pan y en ese momento rompen la luna de nuestro coche y nos roban el portátil. ¿Que ocurre con los datos allí guardados?, puede haber informes y datos de nuestros clientes y también certificados, credenciales, usuarios y contraseñas que permitan acceder a nuestros sistemas.

Los sistemas que puedan salir de nuestra empresa o que puedan ser fácilmente robados (un portátil, un móvil, una tablet...) deben tener los datos cifrados y protegidos por contraseñas fuertes, biometría o incluso tarjetas PKI (tarjetas criptográficas).

Protección física

Uno de los grandes valores de nuestra empresa es el conocimiento. Mucho de este conocimiento estará almacenado en nuestros servidores o en los equipos de los trabajadores. Es necesario hacer una buena proyección física de estos equipos y su información. Esto implica copias de seguridad distribuidas geográficamente o sistemas de apagado de incendios que no dañen a los equipos.

Además es importante disponer de una buena seguridad física que nos prevenga de vandalismos.

Por ejemplo el centro de datos donde no hay personas, se suele usar argón como sistema de extinción de incendios. Cuidado porque este gas desplaza al oxígeno y nos dejaría inconscientes en pocos segundos...

Contraseñas

Las contraseñas deben ser fuertes, complicadas de averiguar, deben contar al menos con ocho caracteres combinando mayúsculas, minúsculas, números y caracteres especiales. También es recomendable evitar el uso de combinaciones típicas fácilmente detectables, pero ¿y eso cómo se hace? Con herramientas que cotejan la contraseña introducida contra una base de datos o diccionario.

Nunca debemos usar las contraseñas por defecto, ni si quiera en entornos de desarrollo y es fundamental implantar una gestión de contraseñas (fecha de caducidad, formato que deben tener...).

Autenticación de segundo y tercer factor

Una contraseña es un buen recurso, pero ante robos de contraseñas, por keyloggers, spyware, etc. estaremos desprotegidos. ¿Cómo podemos añadir una capa más de seguridad? Con la autenticación en varios pasos.

El doble factor de autenticación (2FA), que conviene distinguir de la verificación en dos pasos, es una medida de seguridad que añadirá una capa extra de protección al sistema de autenticación, ya que requiere, además de la propia contraseña del servicio, es decir "algo que sé", de otro mecanismo independiente para comprobar la identidad "algo que soy", por ejemplo una huella digital o el iris, o "algo que tengo" como las llaves de seguridad o los tokens criptográficos, etc.

OSINT

Inteligencia de fuentes abiertas u «Open Source Intelligence» (OSINT) hace referencia al conocimiento recopilado a partir de fuentes de acceso público. El proceso incluye la búsqueda, selección y adquisición de la información, así como un posterior procesado y análisis de la misma con el fin de obtener conocimiento útil y aplicable en distintos ámbitos.

Existen multitud de fuentes abiertas a partir de las cuales se puede obtener información relevante, como redes sociales, medios de comunicación, conferencias, bases de datos o censos públicos...

Phishing

El phishing tradicional consiste en que el cibercriminal se hace pasar por un tercero de confianza para lograr extraer de la víctima su información personal o credenciales de acceso a una plataforma concreta. Normalmente la víctima recibe un correo electrónico donde se le reclama información personal o bien con un enlace que apunta a un sitio malicioso con apariencia real y legítima.

Angler o Social Media Phishing

Los ciberdelincuentes se aprovechan de que las empresas y organizaciones cada vez utilizan más las redes sociales para estar en contacto con sus usuarios, promocionarse, etc. Entonces gracias a ello pueden captar la atención de la víctima. Se hacen pasar por el perfil oficial de una empresa y pueden pedir datos personales a los usuarios, obtener información, enviar links para que inicien sesión, etc.

Clickjacking

En los botones legítimos de una página web que ha sido manipulada se ponen enlaces para descargar malware o es directamente código malicioso.

Clone Phishing

Ataque de phishing donde el atacante copia un mensaje legítimo de correo electrónico que es enviado desde una organización de confianza. El mensaje es alterado añadiendo o reemplazando un enlace que nos lleva a un sitio malicioso.

Malware-based

Correos maliciosos con archivos adjuntos que contienen una pieza de malware o bien un link que apunta a dicho malware.

Pharming

Los archivos hosts de una empresa son manipulados como resultado la solicitudes de ciertas direcciones nos llevan a una URL falsa.

Otra modalidad se basa en DNS spoofing. Esto consiste en que cuando llega una petición para averiguar qué IP está asociada con un nombre, si no usamos protocolos seguros como DNSSEC - DNS Security Extensions - , un atacante podría envenenar la petición con respuestas falsas que nos lleven a una página que nos roba nuestras credenciales al introducirlas. Esto es especialmente fácil en WiFi públicas o creando un WiFi Honeypot.

Phishing en buscadores

Los ciberdelincuentes incluyen anuncios o consiguen posicionar una Web manipulada (SEO) en los principales motores de búsqueda de manera que se hacen pasar por otras páginas que se dedican realmente a ese negocio. Recolectan nuestras credenciales y/o datos bancarios.

Pop-up Phishing

Los cibercriminales infectan páginas legítimas con código malicioso que genera ventanas emergentes cuando las visitamos. En esas ventanas emergentes está el malware o enlace al mismo.

Smishing

Esta amenaza se produce cuando el cliente recibe un mensaje de texto, donde el emisor se hace pasar por el banco, y le informan que se ha realizado una compra sospechosa con su tarjeta de crédito. A su vez, el texto solicita que se comunique con la banca por teléfono de la entidad financiera y le brinda un número falso. El cliente devuelve la llamada y es ahí cuando el ciberdelincuente, haciéndose pasar por el banco, solicita información confidencial para supuestamente cancelar la

compra. En una variante de esta modalidad el mensaje también podría incluir un enlace a una 'web' fraudulenta para solicitar información sensible.

Otro ejemplo: llega un mensaje para engañar a la víctima con que ha ganado un premio o ofreciéndole a participar en un sorteo todo acompañado de un link donde está la Web fraudulenta.

Spear Phishing

Ataque muy personalizado que incluso y puede incluir nombre de la víctima y otros datos lo que hace caer fácilmente en la trampa.

Spray and Pray

Suplanta la identidad bancaria o hacen creer que hemos ganado un premio. Suelen ser correos poco elaborados pero masivos, dirigidos a una gran cantidad de víctimas.

Vishing

De la unión de 'voice' y 'phishing' y se refiere al tipo de amenaza que combina una llamada telefónica fraudulenta con información previamente obtenida desde internet.

Este método consta de dos pasos. Primero, el ciberdelincuente tiene que haber robado información confidencial a través de un correo electrónico o web fraudulenta ('phishing'), pero necesita la clave SMS o token digital para realizar y validar una operación. Es en este momento en que se produce el segundo paso: el ciberdelincuente llama por teléfono al cliente identificándose como personal del banco y, con mensajes particularmente alarmistas, intenta de que el cliente revele el número de su clave SMS o token digital, que son los necesarios para autorizar transacciones.

Watering hole Phishing

Se trata de un ataque avanzado contra organizaciones en la que el atacante infecta con malware sitios web de terceros muy utilizados por los trabajadores de la misma, así cuando estos acceden a dichos sitios webs quedan infectados.

Whaling o Fraude del CEO

Consiste en suplantar la identidad del CEO de una organización y así atacar directamente a los altos ejecutivos u otras personas importantes dentro de ella, con el objeto de robar dinero, conseguir información confidencial u obtener acceso a sus sistemas de información.

2.9 Malwares

"To call up a demon you must learn its name."

"Para invocar a un demonio necesitas conocer su nombre".

— William Gibson, Neuromancer

Estamos acostumbrados a pensar que este término hace referencia a los virus informáticos pero no es sólo eso. Llamamos **malware** a todo tipo de componente software malicioso destinado a causar algún tipo de daño o beneficio fraudulento a través de un ordenador, dispositivo móvil, red de ordenadores, servicio de internet.

El malware emplea además técnicas de evasión para evitar que podamos detectarlos e incluso analizarlos, escondiéndose de antivirus, cortafuegos, gestores de procesos, analizador de tráfico de red, o incluso funcionando en un entorno virtualizado.

2.9.1 Adware

Malware creado con el fin de mostrar anuncios en pantalla. Normalmente suele asociarse al navegador Web. El fin del **adware** es generar ingresos para su propietario, que gana dinero cada

vez que usted hacemos clic en alguno de los anuncios mostrados. Como hace un seguimiento de su navegación, puede presentar anuncios dirigidos y adaptados a nuestros intereses. También puede vender nuestros datos de navegación a terceros. Además, no se detiene si cambia de navegador: el adware reside en el propio sistema operativo, por lo que los anuncios seguirán ahí, no importa la aplicación que utilice para navegar.

2.9.2 Gusano

Los gusanos son en realidad una subclase de virus, por lo que comparten características. Son programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador.

El objetivo de este malware suele ser colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios. A diferencia de los virus, los gusanos no infectan archivos.

2.9.3 Keylogger

Los keyloggers realizan un seguimiento y registran cada tecla que se pulsa en un ordenador, a menudo sin el permiso ni el conocimiento del usuario. Un keylogger puede estar basado en hardware o software, y se puede usar como herramienta lícita de control de TI, tanto profesional como personal. Sin embargo, los keyloggers también se pueden utilizar con fines delictivos. Por regla general, los keyloggers son un spyware malicioso que se usa para capturar información confidencial, como contraseñas o información financiera que posteriormente se envía a terceros para su explotación con fines delictivos.

2.9.4 Ransomware

El malware de rescate, o ransomware, es un tipo de malware que impide a los usuarios acceder a su sistema o a sus archivos personales y que exige el pago de un rescate para poder acceder de nuevo a ellos. Las primeras variantes de ransomware se crearon al final de la década de los 80, y el pago debía efectuarse por correo postal. Hoy en día los creadores de ransomware piden que el pago se efectúe mediante criptomonedas o tarjetas de crédito.

2.9.5 Rogue Software

El rogue software, software bandido o también falso antivirus, es un tipo de programa informático malicioso cuya principal finalidad es la de hacer creer que una computadora es infectada por algún tipo de virus, haciendo pagar al usuario por la licencia completa de un software falso.

El objetivo es claro y sencillo, vender la mayor cantidad de copias de sus falsos productos que sea posibles hasta que los descubran y tengan que volver a rediseñar sus sitios con otros nombres para estos y para sus programas.

2.9.6 Rootkit

Un rootkit es un paquete de software diseñado para permanecer oculto en su equipo mientras proporciona acceso y control remotos. Los hackers utilizan los rootkits para manipular un equipo sin el conocimiento ni el consentimiento del propietario.

La primera parte, «root» (raíz), se refiere a la cuenta de administrador de un dispositivo. Dado que esta cuenta puede acceder a todos los aspectos del dispositivo y dispone de todos los privilegios, disfruta del nivel de control más profundo, como las raíces de una planta. Los rootkits permiten al hacker «echar raíces» en el sistema, como un árbol en busca de nutrientes.

La parte «kit» representa el modo en que se desbloquea este acceso root: mediante un paquete (kit) de software que concede al hacker el control administrativo. El hacker crea un kit de software que le concede privilegios de nivel root sobre el sistema atacado.

2.9.7 Spyware

Software malicioso que infecta su ordenador o dispositivo móvil y recopila información sobre usted, su navegación y su uso habitual de Internet, así como otros datos para luego venderlos.

Troyano

Se denomina caballo de Troya, o troyano, a un malware que se presenta al usuario como un programa aparentemente legítimo e inofensivo, pero que, al ejecutarlo, le brinda a un atacante acceso remoto al equipo infectado.

2.9.8 Virus

El objetivo de un virus es infectar un equipo generando algún tipo de alteración en su comportamiento. El primer virus informático conocido, Creeper, en 1972, se limitaba a sacar un molesto mensaje al usuario.

Funciona como un virus biológico, de hecho, toma su nombre de él.

Busca un huésped en forma de archivo, tradicionalmente infectaba archivos EXE (ejecutables de Windows), pero también hay virus que infectan a otros tipos de archivos, en forma de macro de como archivos de hoja de cálculo, procesador de textos, etc.

Para protegernos de ellos hay que entender cómo funcionan, en este sentido, sabemos que el virus necesita intervención del usuario para ejecutar el archivo portador, por eso la mejor medida de protección es no ejecutar o abrir archivos cuya procedencia sea dudosa.

Muchos servicios de correo ya integran sus propios motores antivirus, luego donde debemos tener cuidado es con los archivos descargados de internet así como los compartidos por pendrive o carpetas en la red local. En estos últimos casos deberíamos siempre usar un antivirus antes de abrir cualquier tipo de archivo (desde un PDF hasta un ejecutable).

2.9.9 Externalización de la ciberseguridad

Los servicios de gestión de seguridad implican un coste adicional a la empresa debido a la contratación de personal con conocimientos avanzados, software y hardware especializado, por lo que en ocasiones es más fácil para las empresas externalizar.

Hablamos de los MSSP (Managed Security Service Provider o Proveedor de Servicios Gestionados de Seguridad), encargados de ayudar a las corporaciones en la compleja tarea de proporcionar servicios de seguridad para mantener sus infraestructuras e información a salvo bajo un mismo paradigma.

El MSSP se encarga de salvaguardar la seguridad de toda organización prestando servicios que van desde el básico antivirus y antispam, hasta el firewall gestionado, la monitorización para la detección de intrusos, exploración de vulnerabilidades, servicios de pentesting y hacking ético, servicios de consultoría, SIEM, SOC, etc.

Disponer de los servicios prestados por un MSSP permite a las empresas disponer de acceso a profesionales de la ciberseguridad altamente capacitados y con experiencia, sin necesidad de invertir para contratar, capacitar y retener el talento en este campo.

Además, el grado de especialización y dedicación del MSSP le permite proporcionar inteligencia de amenazas, ofrecer una detección más rápida y precisa de las amenazas, una rápida respuesta a los ataques y capacidad de auditoría forense.

II Segunda Parte

3 Normativa. Políticas y Auditorías 37

3.1 El sistema de gestión de incidentes
3.2 Plan Director de Seguridad
3.3 Marcos de referencia en gestión de la ciberseguridad
3.4 Normativa de referencia
3.5 Requisitos legales (compliance)
3.6 Auditorías
3.7 Certificaciones Oficiales

4 Plan de prevención y concienciación. 55

4.1 Prevención
4.2 Compliance (cumplimiento normativo)

5 Taxonomía de los incidentes de ciberseguridad 57

5.1 Contenido Abusivo
5.2 Código Malicioso
5.3 Recolección de información
5.4 Intento de intrusiones
5.5 Intrusiones
5.6 Disponibilidad
5.7 Seguridad y confidencialidad de la información
5.8 Fraude
5.9 Vulnerabilidades
5.10 Otros
5.11 Bibliografía para ampliar

3. Normativa. Políticas y Auditorías

> El control a veces puede ser una ilusión. Pero a veces necesitas la ilusión para obtener control. -Mr Robot.

Tener un plan de respuesta a incidentes (IRP) puede marcar la diferencia cuando se responde a un incidente de seguridad. Tener un plan bien documentado para el personal de TI y de seguridad puede asegurar que el proceso de respuesta sea claro y definido, evitando la confusión que le cuesta a la organización un tiempo valioso. Los planes de respuesta a incidentes deben actualizarse constantemente y debe mantenerse una capacitación constante para garantizar que todos los empleados que podrían participar en la respuesta a incidentes sean capaces de desempeñar sus funciones.

3.1 El sistema de gestión de incidentes

Un Sistema de Gestión de la Seguridad de la Información (SGSI o ISMS - Information Security Management System) es un conjunto de políticas de administración de la información.

El concepto clave de un SGSI es el diseño, implantación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vezlos riesgos de seguridad de la información.

Para abordar la ciberseguridad de la empresa es decisivo disponer de un sistema de gestión de incidentes.

3.2 Plan Director de Seguridad

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

A esta planificación la llamaremos Plan Director de Seguridad. Contendrá los proyectos que vamos a abordar tanto técnicos como de contenido legal y organizativos. Así, habrá proyectos de instalación de productos o de contratación de servicios, pero otros serán para cumplir con las leyes de privacidad y comercio electrónico, formar a los empleados o para poner en marcha procedimientos y políticas internas.

Como cada empresa es un mundo, tendremos que calcular nuestro particular nivel de seguridad que será nuestro punto de partida y fijarnos un objetivo de dónde queremos estar. Este objetivo y los proyectos a aplicar siempre tendrán que estar alineados con las estrategias de negocio. Qué vamos a proteger, cómo haremos la prevención, qué incidentes podríamos tener, cómo nos preparamos para reaccionar, etc. Fijamos el punto de partida evaluando el riesgo que nos afecta y el que podemos tolerar. Para el resto pondremos medidas a través de los proyectos, a nuestro ritmo, pero siempre midiendo el progreso en nuestro Plan.

El plan de respuesta a incidentes de INCIBE comprende las siguientes fases:

- Preparación
- Identificación
- Contención
- Erradicación
- Recuperación
- Recapitulación

3.2.1 Preparación

Se puede decir que es la etapa más importante y que requiere la mayor atención, no sólo al redactar el plan, sino también para garantizar que los miembros del equipo reciban una formación continua sobre sus responsabilidades. Podemos dividir esta sección en tres fases principales:

1. Desarrollo de planes de respuesta para diferentes tipos de incidentes y ejecución de escenarios simulados para evaluar cómo responde el equipo de respuesta a los incidentes, entrenándolos para la realidad.
2. Asegurarse de que todos los recursos que necesita el equipo de respuesta a incidentes están aprobados y listos para ser utilizados, tales como: computadoras portátiles, notebooks, herramientas de software, equipo forense, capacitación y la capacidad de abandonar las responsabilidades normales cuando ocurre un incidente.
3. Capacitar y evaluar continuamente el desempeño de los miembros del equipo de respuesta a incidentes para asegurar que sean capaces de cumplir con sus deberes definidos en los planes de respuesta. En el caso de los analistas de seguridad, esto podría consistir en analizar y reunir información sobre el incidente, en el caso de los analistas forenses, en la adquisición y conservación de pruebas digitales, y en el caso de los empleados de los departamentos de relaciones públicas/comunicaciones, en la redacción de notificaciones a la prensa o a las partes interesadas afectadas.

3.2.2 Identificación

Esta sección se centra en la capacidad de identificar y analizar un incidente. Proporcionará una guía sobre cómo reportar un incidente, y qué información debe ser recopilada e incluida, como por ejemplo:

1. ¿Cuándo ocurrió el incidente?
2. ¿Quién lo descubrió?
    1. un miembro del equipo de seguridad
    2. otro empleado que ha reportado una actividad inusual

3. ¿Cómo lo descubrieron?
4. ¿Qué sistemas o unidades de negocio se han visto afectados?
5. ¿Afecta a la capacidad de funcionamiento de la organización?
6. ¿Cuál es el alcance del incidente?
    1. ¿Cuántos sistemas están afectados?
    2. ¿Cuál fue el punto de entrada inicial?
    3. ¿Qué daños se han producido?

Una vez descubierto un incidente, las organizaciones pueden optar por asignar dos valores para ayudar a la priorización, especialmente si se producen varios incidentes simultáneamente:

1. ¿Cómo de crítico es el problema?
2. ¿Qué tan rápida debe ser la respuesta?
3. ¿Qué procesos productivos afectará?
4. ¿Cuánto tiempo impactará el incidente en las operaciones comerciales?

3.2.3 Contención

Es crucial contener un incidente para que no pueda extenderse y afectar a más sistemas causando daños e interrupciones adicionales. Esta sección del IRP debería esbozar las acciones que se deben tomar para contener el incidente tomando medidas como: desconectar los dispositivos comprometidos de Internet evitando el acceso remoto o apagando los sistemas.

Esta etapa es sumamente importante, ya que es el momento en que se recogen y preservan las pruebas digitales para su posterior análisis, por lo que las medidas de contención deben considerarse cuidadosamente, ya que el apagado de un sistema daría lugar a la pérdida de pruebas cruciales que podrían estar en zonas volátiles como la memoria. Se deben documentar directrices y procedimientos cuidadosos para permitir la adquisición de pruebas directas y medidas de contención, tanto a corto como a largo plazo.

Se deben mantener copias de seguridad para que los sistemas afectados puedan ser retirados y las copias de seguridad puedan utilizarse en su lugar, permitiendo así que continúen las operaciones comerciales normales.

3.2.4 Erradicación

Ahora que el incidente no puede extenderse a otros sistemas, se pueden realizar actividades de análisis para averiguar exactamente lo que ocurrió. El marco de MITRE ATT&CK puede ser usado para trabajar hacia atrás y potencialmente identificar pasos previos del ataque. El análisis se llevará a cabo utilizando métodos tales como mirar las capturas de paquetes, revisar los registros de un SIEM y trabajar hasta que se haya identificado la causa de fondo. Se deben proporcionar directrices que indiquen cómo se debe realizar el análisis y se deben proporcionar los recursos apropiados, como herramientas de software.

Una vez encontrados, es hora de empezar a eliminar los artefactos maliciosos como la presencia de malware, cualquier cambio en los sistemas y configuraciones realizado por los agentes maliciosos, y asegurar que se elimine cualquier método para retener la persistencia de manera que los agentes no puedan volver a entrar en los sistemas.

En este punto se deben tomar medidas defensivas para asegurar que este tipo de incidente no pueda volver a ocurrir mediante el endurecimiento de los sistemas, la aplicación de parches y la potenciación de las defensas automatizadas como el NIPS y el HIPS utilizando indicadores de compromiso reunidos a lo largo de la investigación. Mediante la creación de libros de registro de diferentes incidentes, los responsables de la respuesta a los incidentes pueden evaluar rápidamente las medidas sugeridas e implementarlas rápidamente para evitar que ocurran incidentes adicionales.

3.2.5 Recuperación

Esta etapa consiste en volver a la normalidad de las operaciones comerciales trasladando los sistemas afectados a los entornos de producción ahora que han sido limpiados y endurecidos. Se deben proporcionar directrices para asegurar que los sistemas ya no están infectados, y cómo devolverlos adecuadamente a las operaciones comerciales. Un ejemplo de esto podría ser un sitio web que ha sido comprometido a través de web shells, dando a los atacantes acceso al propio servidor. En este caso, se podría utilizar un servidor de respaldo para alojar el sitio principal temporalmente. Una vez que el servidor infectado se ha limpiado y se ha eliminado toda presencia maliciosa, el sitio puede volver a alojarse en el servidor principal.

3.2.6 Recapitulación

Una vez que se hayan completado la investigación y la respuesta, se debe celebrar una reunión que incluya a todas las partes interesadas en el incidente. El objetivo de esta reunión debería ser recapitular exactamente lo que sucedió, específicamente lo que salió bien, y cómo se podría haber mejorado la respuesta. Las enseñanzas extraídas tanto de los acontecimientos simulados como de los reales ayudarán a fortalecer los sistemas contra cualquier ataque futuro.

Los puntos fuertes y débiles de la respuesta deben ser discutidos y utilizados para impulsar el cambio, como por ejemplo reescribir la documentación, incluyendo las políticas y procedimientos, o asegurar más presupuesto si es necesario para herramientas o personal adicional.

Pasar por un incidente puede ser duro, pero aprender de los errores y las lagunas en la seguridad puede permitir al equipo de seguridad mejorar las defensas y elevar la postura de seguridad de la organización. Un plan eficaz de respuesta a incidentes debe actualizarse constantemente para que siga siendo un recurso válido y útil.

También es necesario completar la capacitación de manera rutinaria para que los miembros del equipo de respuesta a incidentes sigan siendo eficaces y estén preparados para ponerse a trabajar. Los ejercicios de mesa y los ataques simulados pueden ser una gran herramienta para mantener un alto nivel de preparación, con la participación de todos los interesados apropiados.

Para más información podemos consultar estas guías:

- Guía de respuesta a incidentes.
- Plan director de seguridad.

3.3 Marcos de referencia en gestión de la ciberseguridad

“Hacerte invencible significa conocerte a ti mismo” El Arte de la Guerra Sun Tzu

3.3.1 El CTN 320

El comité de expertos del CTN 320, de la Asociación Española de Normalización, se encarga de la normalización de los métodos, técnicas y directrices en el ámbito de la ciberseguridad, la seguridad de la información, las comunicaciones y las TI, lo que incluye las siguientes áreas:

- Metodología para la captura de requisitos.
- Técnicas y mecanismos de seguridad, incluidos los procedimientos para el registro de los componentes de seguridad.
- Gestión de la ciberseguridad, la seguridad de la información, las comunicaciones y las TI.
- Documentación de apoyo a la gestión, incluyendo las normas relativas a la terminología, la evaluación de la conformidad y los criterios de evaluación de la seguridad.
- Los requisitos y directrices para la protección de los datos personales y la privacidad de las personas, incluyendo los aspectos de gestión y requisitos de privacidad por diseño y por

defecto.

El comité tiene la siguiente estructura:

- SC1 Sistemas de gestión de la ciberseguridad
- SC2 Criptografía y mecanismos de seguridad
- SC3 Evaluación, pruebas y especificaciones de seguridad
- SC4 Controles y servicios de seguridad
- SC5 Protección de datos, privacidad y gestión de la identidad
- SC6 Seguridad de los productos

Este comité, se ha encargado de elaborar las siguientes normas:

- UNE-EN ISO/IEC 27007:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Directrices para la auditoría de los sistemas de gestión de la seguridad de la información (ISO/IEC 27007:2020) (Ratificada por la Asociación Española de Normalización en febrero de 2022.)
- UNE-EN ISO/IEC 27000:2021. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Visión de conjunto y vocabulario. (ISO/IEC 27000:2018).
- UNE-EN ISO/IEC 27701:2021. Técnicas de seguridad. Extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de privacidad de la información. Requisitos y directrices. (ISO/IEC 27701:2019).
- UNE-EN ISO/IEC 29101:2021. Tecnología de la información. Técnicas de seguridad. Marco de arquitectura de la privacidad (ISO/IEC 29101:2018) (Ratificada por la Asociación Española de Normalización en noviembre de 2021.)
- UNE-EN ISO/IEC 15408-3:2020. Tecnología de la información. Técnicas de seguridad. Criterios de evaluación para la seguridad de TI. Parte 3: Componentes de aseguramiento de la seguridad (ISO/IEC 15408-3:2008, Versión corregida 2011-05) (Ratificada por la Asociación Española de Normalización en mayo de 2020.)
- UNE-EN ISO/IEC 27006:2020. Tecnología de la información. Técnicas de seguridad. Requisitos para organismos que realizan auditorías y certificación de sistemas de gestión de seguridad de la información (ISO/IEC 27006:2015, incluyendo Amd 1:2020) (Ratificada por la Asociación Española de Normalización en enero de 2021.)
- UNE-EN ISO/IEC 27017:2021. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información basados en la norma ISO/IEC 27002 para los servicios en nube. (ISO/IEC 27017:2015). (Ratificada por la Asociación Española de Normalización en marzo de 2021.)
- UNE 320002:2021. Arquitecturas de Confianza para el Intercambio de Inteligencia de Ciberamenazas.
- UNE 320001:2021. Metodología de evaluación LINCE para la ciberseguridad de productos TIC.
- UNE 71510:2011. Aplicaciones con Documento Nacional de Identidad electrónico (DNIe). Creación y verificación de firma electrónica. Tipo 1 para plataformas de Tecnologías de la Información (TI) que permiten un control exclusivo de los interfaces con el firmante, y con un nivel de garantía de evaluación «EAL1».
- UNE 71511:2011. Aplicaciones con Documento Nacional de Identidad electrónico (DNIe). Creación y verificación de firma electrónica. Tipo 1 para plataformas de Tecnologías de la Información (TI) que permiten un control exclusivo de los interfaces con el firmante, y con un nivel de garantía de evaluación «EAL3».
- UNE 71512:2011. Aplicaciones con Documento Nacional de Identidad electrónico (DNIe).

Creación y verificación de firma electrónica. Tipo 2 para ordenadores personales, y con un nivel de garantía de evaluación «EAL1».

- UNE 71513:2011. Aplicaciones con Documento Nacional de Identidad electrónico (DNIe). Creación y verificación de firma electrónica. Tipo 2 para ordenadores personales, y con un nivel de garantía de evaluación «EAL3».
- UNE-ISO/IEC TR 19791:2013 IN. Tecnologías de la información. Técnicas de seguridad. Evaluación de la seguridad de sistemas operacionales.
- UNE-EN ISO/IEC 19790:2020. Tecnología de la información. Técnicas de seguridad. Requisitos de seguridad para módulos criptográficos (ISO/IEC 19790:2012, incluyendo versión corregida 2015-12) (Ratificada por la Asociación Española de Normalización en mayo de 2020.)
- UNE-EN ISO/IEC 29100:2020. Tecnología de la información. Técnicas de seguridad. Marco de privacidad. (ISO/IEC 29100:2011, incluyendo Amd 1:2018) (Ratificada por la Asociación Española de Normalización en julio de 2020.)
- UNE-EN ISO/IEC 27018:2020. Tecnología de la Información. Técnicas de seguridad. Código de práctica para la protección de identificación personal (PII) en nubes públicas que actúan como procesadores PII (ISO/IEC 27018:2019) (Ratificada por la Asociación Española de Normalización en julio de 2020.)
- UNE-EN ISO/IEC 27011:2020. Tecnología de la información. Técnicas de seguridad. Código de prácticas para los controles de la seguridad de la información basados en la ISO/IEC 27002 para los organismos de telecomunicaciones (ISO/IEC 27011:2016) (Ratificada por la Asociación Española de Normalización en julio de 2020.)
- UNE-EN ISO/IEC 29147:2020. Tecnología de la información. Técnicas de seguridad. Divulgación de la vulnerabilidad (ISO/IEC 29147:2018) (Ratificada por la Asociación Española de Normalización en julio de 2020.)
- UNE-EN ISO/IEC 30111:2020. Tecnología de la información. Técnicas de seguridad. Procesos de manejo de vulnerabilidades (ISO/IEC 30111:2019) (Ratificada por la Asociación Española de Normalización en julio de 2020.)
- UNE-EN ISO/IEC 27019:2020. Tecnología de la información. Técnicas de seguridad. Controles de seguridad de la información para la industria de servicios de energía (ISO/IEC 27019:2017, versión corregida 2019-08) (Ratificada por la Asociación Española de Normalización en mayo de 2020.)
- UNE-EN ISO/IEC 15408-1:2020. Tecnología de la información. Técnicas de seguridad. Criterios de evaluación para la seguridad de TI. Parte 1: Introducción y modelo general (ISO/IEC 15408-1:2009) (Ratificada por la Asociación Española de Normalización en mayo de 2020.)
- UNE-EN ISO/IEC 15408-2:2020. Tecnología de la información. Técnicas de seguridad. Criterios de evaluación para la seguridad de TI. Parte 2: Componentes funcionales de seguridad (ISO/IEC 15408-2:2008) (Ratificada por la Asociación Española de Normalización en mayo de 2020.)
- UNE-EN ISO/IEC 29134:2020. Tecnología de la información. Técnicas de seguridad. Directrices para la evaluación del impacto de la privacidad (ISO/IEC 29134:2017) (Ratificada por la Asociación Española de Normalización en mayo de 2020.)
- UNE-EN ISO/IEC 18045:2020. Tecnología de la información. Técnicas de seguridad. Metodología para la evaluación de la seguridad TI (ISO/IEC 18045:2008).
- UNE-EN ISO/IEC 27002:2017. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información. (ISO/IEC 27002:2013

incluyendo Cor 1:2014 y Cor 2:2015).

- UNE-EN ISO/IEC 27001:2017. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015)
- UNE-EN ISO/IEC 27042:2016. Tecnología de la información. Técnicas de seguridad. Directrices para el análisis y la interpretación de las evidencias electrónicas (ISO/IEC 27042:2015) (Ratificada por AENOR en diciembre de 2016.)
- UNE-EN ISO/IEC 27041:2016. Tecnología de la información. Técnicas de seguridad. Directrices para garantizar la idoneidad y adecuación del método de investigación de incidentes (ISO/IEC 27041:2015).
- UNE-EN ISO/IEC 27037:2016. Tecnología de la información. Técnicas de seguridad. Directrices para la identificación, recogida, adquisición y preservación de evidencias electrónicas (ISO/IEC 27037:2012).
- UNE-EN ISO/IEC 27038:2016. Tecnología de la información. Técnicas de seguridad. Especificación para la redacción digital (ISO/IEC 27038:2014).
- UNE-EN ISO/IEC 27043:2016. Tecnología de la información. Técnicas de seguridad. Principios y procesos de investigación de incidentes (ISO/IEC 27043:2015).
- UNE-EN ISO/IEC 27040:2016. Tecnología de la información. Técnicas de seguridad. Seguridad en el almacenamiento (ISO/IEC 27040:2015).
- UNE 71506:2013. Tecnologías de la Información (TI). Metodología para el análisis forense de las evidencias electrónicas.
- UNE 71505-1:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 1: Vocabulario y principios generales.
- UNE 71505-2:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas.
- UNE 71505-3:2013. Tecnologías de la Información (TI). Sistema de Gestión de Evidencias Electrónicas (SGEE). Parte 3: Formatos y mecanismos técnicos.
- UNE-ISO/IEC TR 15446:2013 IN. Tecnologías de la información. Técnicas de seguridad. Guía para la producción de perfiles de protección y objetivos de seguridad.

3.3.2 La serie ISO/IEC 27000

La ISO o International Organization for Standardization dispone de productos que son reconocidos estándares internacionales, basados en informes técnicos y que recogen especificaciones técnicas, disponibles públicamente disponibles en forma de guías.

Entre las ventajas de usar una norma internacional están:

- Identificar los riesgos y establecer controles para gestionarlos o eliminarlos
- Flexibilidad para adaptar los controles a todas las áreas de su empresa o solo a algunas seleccionadas
- Conseguir que las partes interesadas y los clientes confíen en la protección de los datos
- Demostrar conformidady conseguir el estatus de proveedor preferente
- Cumplir con más requisitos demostrando conformidad

Estándares de seguridad de la información:

- ISO/IEC 27000. Es un vocabulario estándar para el SGSI.
- ISO/IEC 27001. Norma que especifica los requisitos para la implantación del SGSI.
- ISO/IEC 27002. Código de prácticas para la gestión de la seguridad de la información.
- **ISO/IEC 27003. Son directrices para la implementación de un SGSI.**
- ISO/IEC 27004. Son métricas para la gestión de seguridad de la información.

- ISO/IEC 27005. Gestión de riesgos en seguridad de la información.
- ISO/IEC 27006. Requisitos de acreditación de organizaciones.
- **ISO/IEC 27007. Es una guía para auditar los controles a implantar un SGSI.**
- ISO/IEC 27008. Es una guía para auditar al SGSI.
- ISO/IEC 27010. Es una guía para gestionar la seguridad de la información compartida.
- ISO/IEC 27014. Es una guía de gobierno corporativo de la seguridad de la información.
- ISO/IEC 27017. Es una guía de seguridad para cloud computing.
- **ISO/IEC 27032. Es una guía para fortalecer la ciberseguridad en una empresa.**
- ISO/IEC 27033. Es una guía de seguridad para la administración, operación y uso de redes.
- ISO/IEC 27034. Es una referencia sobre técnicas de seguridad y seguridad de aplicaciones.
- ISO/IEC 27036. Seguridad de la información para las relaciones con los proveedores.
- ISO/IEC 27039. Guía para el despliegue de sistemas de detección y prevención de intrusión.
- ISO/IEC 27042. Guía para el análisis e interpretación de las evidencias digitales.

Para cualquier norma 27000 que queramos implantar, es necesario:

1. Compromiso de los niveles directos.
2. Participación colectiva. Que toda la empresa participe con una buena comunicación interna.
3. Comparar la Gestión de la Seguridad de la Información actual con los requisitos de la norma.
4. Consultar opiniones de clientes y proveedores sobre el sistema actual de Gestión de Seguridad de la Información.
5. Definir equipos de trabajo. Establezca un equipo de implantación.
6. Reparto. Asigne y comparta funciones, responsabilidades y plazos.
7. Adaptación. Adapte los principios básicos de la norma ISO/IEC 27001 a su empresa.
8. Motivación. Fomente la implicación del personal con formación e incentivos.
9. Comunicación. Comparta sus conocimientos de la norma ISO/IEC 27001 y anime al personal a formarse.
10. Revisión continua. Revise con regularidad su sistema ISO/IEC 27001 para asegurarse de que lo continúa mejorando.

La ISO/IEC 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el conocido "Ciclo de Deming": PDCA – acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar), siendo éste un enfoque de mejora continua:

- Plan (planificar): es una fase de diseño del SGSI de evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
- Do (hacer): es una fase que envuelve la implantación y operación de los controles.
- Check (controlar): es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- Act (actuar): en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento. Sistema de Gestión de Seguridad de la Información (estándares internacionales)

El alcance del SGSI aclara los límites del SGSI en función del contexto y/o importancia y ubicación de los activos críticos de información de la organización (por ejemplo, unidades, ubicaciones o departamentos) y los riesgos propios o externos asociados (p.ej. leyes y reglamentos, obligaciones contractuales, estrategias y políticas impuestas por organismos centrales).

3.3.3 ISO 22301

Se trata del primer estándar internacional para la Gestión de la Continuidad del Negocio (BCM), desarrollado para ayudar a las organizaciones a minimizar el riesgo del cese de un negocio o

actividad ante las eventuales interrupciones.

Entre las principales aportaciones de este estándar:

- Mayor énfasis en la definición de objetivos.
- Seguimiento mediante métricas adecuadas.
- Clara definición de las responsabilidades de la Dirección.
- Mejora en la planificacion de los recursos para garantizarla Continuidad del Negocio.

El objetivo de esta norma es:

- Inspirar confianza en su capacidad para continuar las operaciones durante una interrupción.
- Protegersu reputación.
- Responder a los requisitoslegislativos.
- Reducir el costo de la interrupción.
- Crear una ventaja competitiva.
- Contribuir a la resiliencia organizacional.

3.3.4 NIST

El NIST o National Institute of Standards and Technology dispone de una serie de publicaciones especiales que tienen como objetivo promover la innovación y la competencia industrial en Estados Unidos.

Entre otras áreas aborda:

- biotecnología
- nanotecnología
- **tecnologías de la información**
- fabricación avanzada.

Dentro del marco de la ciberseguridad entramos las NIST CSF que son publicaciones especiales que ayudan a proteger tanto infraestructuras críticas de organizaciones del sector privado, como la privacidad y las libertades civiles. Hablamos de la serie 800, donde destacamos (`https://csrc.nist.gov/publications/sp800`):

- 800-12. Es una visión de las áreas de control de ciberseguridad.
- 800-14. Describe los principios de seguridad comunes
  - Proporciona elementos a incorporar en una política de ciberseguridad.
- 800-26. Proporciona consejos de cómo administrar la seguridad de TI.
- **800-30. Guía para la gestión de riesgos.**
- 800-37. Es una guía para aplicar la gestión de riesgos a los sistemas de información.
- 800-53. Sobre controles de seguridad para organizaciones y sistemas de información.
- 800-63-3. Es sobre las pautas de identidad digital
  - Proporciona recomendaciones para implementar servicios de identidad digital.
- 800-82. Guía para la seguridad del sistema de control industrial o ICS.
  - Describe cómo asegurar los sistemas de control industrial contra ciberataques.
- **800-160 Vol. 2 Rev. 1. Guía para desarrollar sistemas ciberresilistentes**.

3.3.5 ITIL

ITIL corresponde a una metodología de gestión que propone una serie de prácticas estandarizadas que nos ayudan a mejorar la prestación de un servicio, reorganizando la manera que tiene la empresa de trabajar y en particular, la del departamento de TI. ITIL - Information Technology Infrastructure Library propone:

1. Estrategia: propone un enfoque de la gestión como una capa estratégica de la compañía, que deja de ser simplemente una burocracia de cumplimentar o acatar.

2. Diseño: cubre los principios y métodos necesarios para transformar los objetivos estratégicos en portafolios de servicios y activos.
3. Transición:se trata del proceso de transición para la implementación de nuevos servicios o de su mejora.
4. Operación: cubre las mejores prácticaspara la gestión rutinaria.
5. Mejora Continua: corresponde a un procedimiento mediante el cual se crea y mantiene del valor ofrecido a los clientes a través de un diseño,transición y operación delservicio optimizado.

3.4 Normativa de referencia

3.4.1 Normativa nacional

A nivel nacional disponemos de las siguientes normas sobre seguridad:

- Ley 36/2015, de 28 de septiembre, de Seguridad Nacional, que regula los principios y organismos clave así como las funciones que deberán desempeñar para la defensa de la Seguridad Nacional.
- Orden TIN/3016/2011, de 28 de Octubre, por la que se crea el Comité de Seguridad de las Tecnologíasde la Información y las Comunicacionesdel Ministerio de Trabajo e Inmigración.
- Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana.
- Ley 5/2014, de 4 de abril, de Seguridad Privada.
- A nivel de incidentes hay una inclusión parcial en la Ley 34/2002, de 11 de julio, de servicios a la sociedad de la información y comercio electrónico.

En lo referente a telecomunicaciones, tenemos:

- Ley 34/2002, de 11 de julio, de servicios a la sociedad de la información y comercio electrónico.
- Real Decreto 381/2015, de 14 de mayo, por el que se establecen medidas contra el tráfico no permitido o irregular con fines fraudulentos en comunicaciones electrónicas.
- Ley 50/2003, de 19 de diciembre, de firma electrónica.
- La Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Para delitos de ciberdelincuencia, encontramos inclusiones parciales en el Código Penal, la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores; o en el Real Decreto de aprobación de la Ley de Enjuiciamiento Criminal.

En cuanto a protección de datos la referencia es la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales* que derogó a la Ley Orgánica 15/1999, de 13 de diciembre y su Reglamento, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

3.4.2 Normativa Europea

A nivel europeo disponemos del Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) n.o 526/2013 («Reglamento sobre la Ciberseguridad»). Con éste se pretende:

- Contribuir a la elaboración y ejecución de la política y del derecho de la Unión.
- Asistir a la creación de capacidades de ciberseguridad.

- Apoyar la cooperación entre los Estados miembros, las instituciones, órganos y organismos de la Unión y entre las partes interesadas.
- Mercado, certificación de la ciberseguridad y normalización.
- Conocimiento e información.
- Sensibilización y educación.
- Investigación e innovación.
- Cooperación internacional.

También a nivel europeo diponemos del conocido Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Hablaremos de él un poco más adelante.

NIS

La Directiva NIS es una normativa de la Unión Europea que busca mejorar la seguridad de las redes y sistemas de informaciónen su territorio. Entró en vigor en agosto de 2017. En España se aprobó en 2018 el real decreto-ley que realizaba la transposición de la directiva europea.

Los Operadores de Servicios Esenciales (OES), designados por la autoridad competente, en función de si prestan un servicio esencial que dependa de redes y sistemas de información, y teniendo en cuenta además si un incidente sobre el servicio pudiera tener efectos perturbadores en la sociedad.

- Los Proveedores de Servicios Digitales (DSP), aquellas entidades que presten un servicio digital (en el sentido recogido en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico (LSSI)).
- Mercados en línea.
- Motores de búsqueda en línea.
- Servicios de computación en la nube.

Esta normativa obliga a comunicar incidencias muy graves y graves a los CSIRT de referencia. Entre los factores a tener en cuenta para notificar una incidencia:

- El número de usuarios afectados.
- La duración del incidente.
- Su extensión.
- El grado de perturbación que origine.
- El alcance del impacto en actividades económicas y sociales cruciales.
- La importancia de los sistemas y el daño a la reputación.

Las sanciones pueden ser leves, graves o muy graves, con una cuantía que podrá llegar hasta 1.000.000€ en función del tipo de sanción, teniendo en cuenta un conjunto de criterios establecidos en la Ley (grado de culpabilidad o la existencia de intencionalidad, continuidad o persistencia en la conducta infractora, naturaleza y cuantía de los perjuicios causados, etc.), aplicando los criterios de proporcionalidad que permitan que la sanción sea lo más justa posible.

Como ya veremos en el tema “Respuesta a Incidentes”, En España los CSIRT de referencia son:

- CCN-CERT: atiende las notificacionesde las entidades de ámbito público.
- Incibe-CERT: recibe las comunicaciones de los operadores críticos y de los proveedores de servicios digitales que no sean públicos. Estambién el CSIRT de referencia para ciudadanos y entidades privadas.
- ESPDEF-CERT: del Ministerio de Defensa, colabora con los dos anteriores en casos de especial necesidad o carácter militar.

3.5 Requisitos legales (compliance)

3.5.1 LOPDGDD

La LOPD GDD o Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales vela por la privacidad de los ciudadanos cuidando la seguridad de datos de carácter personal tanto en formato electrónico como papel. Aplica a empresas y a los que utilizan datos de contacto del personal, es decir tanto propios, como de clientes y de proveedores. El objetivo es reforzar los derechos de los ciudadanos. Puede consultarse en:

`https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf`

Introduce un estándar único de protección de datos coherente con la UE lo que aporta beneficios para las empresas que ya no tendrán que enfrentarse a distintas leyes en los países de la Unión cuando realicen tratamientos de datos personales.

También aporta beneficios para los consumidores al proteger sus derechos de igual forma en toda la **UE Derechos ARCO** (acceso, rectificación, cancelación y oposición).

3.5.2 RGPD

El RGPD o Reglamento General de Protección de Datos Personales de la UE, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales

y a la libre circulación de estos datos.

Los cambios aprobados que afectan a las empresas en líneas generales son:

- Se obliga a ciertas empresas a disponer de un Delegado de Protección de Datos
- Se elimina la necesidad de inscribir los ficheros en la AEPD
- Se incorpora el principio de rendición de cuentas
- Garantiza el cumplimiento de responsabilidades en protección de datos.
- Aumenta las sanciones.

3.5.3 Acceso electrónico de los ciudadanos a los Servicios Públicos

Se trata de un derecho de los ciudadanos recogido en la ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos(LAECSP) que pretende:

- Facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos.
- Facilitar el acceso de los ciudadanos a la información y al procedimiento administrativo.
- Velar por la protección de datos de carácter personal.
- Promover la transparencia administrativa.
- Simplificarlos procedimientos administrativos.

Se basa en los siguientes fundamentos:

- Principio de igualdad con objeto de que en ningún caso el uso de medios electrónicos pueda implicar la existencia de restricciones o discriminaciones para los ciudadanos que se relacionen con las Administraciones Públicas por medios no electrónicos.
- Principio de legalidad en cuanto al mantenimiento de la integridad de las garantías jurídicas de los ciudadanos ante las Administraciones Públicas establecidas en la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.
- Principio de cooperación en la utilización de medios electrónicos por las Administraciones Públicas, debiendo de ser interoperativas y reconocerse mutuamente los documentos electrónicos y los medios de identificación y autenticación.
- Principio de proporcionalidad en cuya virtud sólo se exigirán las garantías y medidas de seguridad adecuadas a la naturaleza y circunstancias de los distintos trámites y actuaciones.

Sólo se requerirán a los ciudadanos aquellos datos que sean estrictamente necesarios.
- Principio de simplificación administrativa para reducir tiempos y plazos en los procedimientos administrativos.

3.5.4 ENS

El Esquema Nacional de Seguridad (ENS) se establece en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica. Comprende:

- Los principios básicos a ser tenidos en cuenta en las decisiones en materia de seguridad.
- Los requisitos mínimos que permitan una protección adecuada de la información.
- La categorización de los sistemas, en nivel Alto Medio o Bajo, para la adopción de medidas de seguridad proporcionales a la naturaleza de la información, del sistema y de los servicios a proteger y a losriesgos a que están expuestos.
- Las medidas de seguridad (75) organizadas en: Marco Organizativo (4), Marco Operacional (31) y Medidas de protección (40)
- La auditoría de la seguridad que verifique el cumplimiento del Esquema Nacional de Seguridad

El ámbito de aplicación del ENS es el de las Administraciones Públicas, los ciudadanos en sus relaciones con las mismas y el de las relaciones entre ellas.

Su objetivo es establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información. Dentro los objetivos del ENS destacan:

- Crear las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de la información y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones Públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la Ley 11/2007, que estará constituida por los principios básicos y los requisitos mínimos para una protección adecuada de la información.
- Introducir los elementos comunes que han de guiar la actuación de las Administraciones públicas en materia de seguridad de lastecnologías de la información.
- Aportar un lenguaje común para facilitar la interacción de las Administraciones públicas, así como la comunicación de los requisitos de seguridad de la información a la Industria.
- Aportar un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios de administración electrónica cuando participan diversas entidades.
- Facilitar un tratamiento continuado de la seguridad.

3.5.5 PIC

Dentro del marco normativo asociado a la ciberseguridad industrial, tiene especial importancia en España la Ley de Protección de Infraestructuras Críticas (Ley PIC 8/2011) complementada por el Real Decreto 704/2011. Los dos grandes objetivos de esta norma son:

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

Además también son de aplicación:

- La Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.
- Real Decreto 704/2011 de 20 de mayo, por el que se aprueba el Reglamento de protección de lasinfraestructuras críticas.

El Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC) es "el órgano responsable del impulso, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las infraestructuras críticas españolas y con la ciberseguridad en el seno del Ministerio del Interior". Entre sus competencias están:

1. Recolectar, analizar, integrar y evaluar la información aportada por las instituciones públicas, los servicios policiales, y sectores estratégicos
2. Evaluar las amenazas y analizar los riesgos sobre las instalaciones estratégicas.
3. Diseñar y establecer la información, la comunicación y los mecanismos de alerta.
4. Coordinar las administraciones españolas con los respectivos programas de la Unión Europea.

El Plan Nacional de Protección de las Infraestructuras Críticas (PNPIC) obliga a que todas las infraestructuras críticas cuenten con un responsable de seguridad que haga de enlace con el Centro Nacional de Protección de lasInfraestructuras Críticas en caso de que sea necesario. También fomenta el intercambio de información entre las diversas empresas e instituciones afectadas por esta catalogación y define las medidas resolutivas que deben de poner en marcha las infraestructuras críticas en caso de ser víctimas de un ataque. Por último, recoge los dictámenes y directivas que sigue el Estado para movilizar sus capacidades operativas frente a ataques deliberados, así como los mecanismos de coordinación establecidos con los operadores críticos en estos casos.

Los responsables de su cumplimiento son:

Responsables

1. Gobiernos – Son los principales interesados en la generación e implantación de iniciativas de Protección de Infraestructuras Críticas para garantizar que los servicios esenciales funcionen de manera adecuada.
2. Organismos competentes – Es muy común que los gobiernos deleguen las tareas de difusión, elaboración y gestión de iniciativas de Protección de Infraestructuras críticas (PIC) en organismos públicos, privados o combinación de ambos.
3. Operadores de infraestructuras críticas – Son los que tienen más interés en que sus infraestructuras sean seguras, funcionen de manera adecuada y no sufran daños, interrupciones ni ataques.
4. Terceras partes – No se ven afectadas de manera directa por las exigencias legales, pero sí manera indirecta. Un ejemplo de ello son las empresas en que los operadores de las infraestructuras hayan delegado la gestión de las mismas.

3.5.6 PSD2

PSD2 (Payment Services Directive) es la Directiva Europea (UE) 2015/2366 que regula los servicios de pago (por ejemplo transferencias, domiciliaciones, pagos con tarjetas...) realizados en Europa con la finalidad de impulsar la transparencia, la competencia, y la innovación de los servicios de pago del sector financiero.

Permite además que terceras empresas (Third Party Providers o TPP), también intervengan en los pagos. Esto es lo que se conoce como open banking.

En España se aprobó el Real Decreto Ley 19/2018 de servicios de pago para transponer esta normativa a nuestro ordenamiento. La norma recoge los derechos y obligaciones de entidades y clientes en materia de servicios de pago. Una cuestión muy relevante es el refuerzo de las medidas de seguridad para realizar estas transacciones incluyendo medidas de doble autenticación

o autentificación reforzada.

3.5.7 HIPAA

La Health Insurance Portability and Accountability Act (HIPAA) es la Ley de Portabilidad y Responsabilidad de Seguros de Salud en Estados Unidos y es usada de manera general para gestión de datos médicos como referencia.

Los profesionales de la salud tienen el deber de tomar medidas razonables para preservar la confidencialidad de la información médica personal, de acuerdo con las preferencias de la persona en cuestión. Por ejemplo, las conversaciones entre médico y paciente deben transcurrir, por lo general, en privado, y es posible que un paciente prefiera que su médico le llame al teléfono móvil en lugar de al teléfono fijo del domicilio. Ni siquiera los familiares bienintencionados están necesariamente autorizados a recibir información sobre la situación médica de un ser querido. La HIPAA dicta que:

- Toda persona debe poder ver y obtener copias de su historial médico y pedir que se corrijan los errores que pueda contener.
- Cualquier persona legalmente autorizada para tomar decisiones relacionadas con la atención médica en nombre de otra persona que carezca de capacidad para ello, tiene el mismo derecho de acceso a la información médica privada que la persona en cuestión.
- Los profesionales de la salud deben dar a conocer regularmente de qué modo garantizan la confidencialidad de la información médica.
- Los profesionales de la salud deben compartir la información médica de una persona, pero solo entre ellos mismos en la medida en que sea preciso para proporcionar los cuidados necesarios.
- La información médica personal no puede ser revelada con fines comerciales.
- Los profesionales de la salud deberán tomar las precauciones necesarias para garantizar la confidencialidad de sus comunicaciones con el paciente.
- Las personas pueden presentar denuncias sobre prácticas de privacidad de los profesionales de la salud (directamente al profesional de la salud o ante el organismo gubernamental correspondiente, en el caso de Estados Unidos en la Oficina de Derechos Civiles del Departamento de Salud y Servicios Humanos

3.6 Auditorías

Las auditorías deben ser llevadas a cabo por personal altamente cualificado, para conseguir una mejora real en eficacia y eficiencia de los procesos.

Los informes de auditoría del SGSI son la evidencia más directa que documenta los principales hallazgos, conclusiones y recomendaciones de la auditoría con la posibilidad de comunicar no conformidades y acciones correctivas, mejoras. Debe garantizarse en una auditoría:

- La imparcialidad.
- La competencia de los profesionales designados.

Distinguimos entre estos tipos fundamentales de auditorías internas de cumplimiento en materia de prevención:

1. Auditoría de sistemas, que tienen como objetivo:
    1. Detallar los elementos clave que queremos que sean auditados.
    2. Identificar los activos esenciales para el negocio.
    3. Revisar si disponen de:
        1. sistemas antimalware.

2. procesos de gestión de permisos procesos de cumplimiento legal
3. políticas de prevención de fraude y de fuga de datos sistema de actualizaciones sistemas de monitorización de recursos

4. Procedimiento:
   1. Análisis de logs y puertos
   2. Análisis de vulnerabilidades
   3. Auditoría de contraseñas
   4. Auditoría de sistemas y ficheros
   5. Auditoría de red
   6. Herramientas de recuperación de datos
   7. Herramientas de comprobación de software/aplicaciones web

2. Auditorías legales, que tienen como objeto garantizar el cumplimiento de los requerimientos legales.
3. Auditorías forenses, que tienen como objetivo identificar causas ante un incidente de seguridad, depurar responsabilidades e iniciar un procedimiento judicial si fuese necesario.

En el caso de la norma 27000, por ejemplo, las no conformidades y acciones correctivas con los requisitos del sistema ayudan a la mejora continua del mismo. El origen de los requisitos es obviamente el estándar ISO/IEC 27001 pero también surgen de las necesidades aplicadas por la propia organización (estrategias, políticas, procedimientos, pautas) o por partes externas a ella (leyes, regulaciones y contratos) en relación a las actividades del alcance del SGSI.

Mantener un registro o índice de no conformidades, junto con la evidencia cuidadosamente presentada de las acciones emprendidas en respuesta a las no conformidades, tales como:

- Reacción inmediata de contención o reparación de la no conformidad.
- Análisis de causa raíz para evitar recurrencias.
- Aplicación y resultados finales de la acción correctiva, incluida la revisión de su efectividad y finalización/cierre/aprobación de la no conformidad.

3.6.1 Procedimientos

- Test de penetración.
- Auditoría de red.
- Auditoría de seguridad perimetral.
- Auditoría web.
- Auditoría forense.
- Auditoría legal.
- Registro de logs y generación de informes.

3.6.2 Herramientas de auditoría

NMAP

FOCA

OpenVAS

Nessus

3.7 Certificaciones Oficiales

3.7.1 ISACA

- CISA
- CISM
- CRISC

3.7.2 (ISC)²

- CISSP (Certified Information Systems Security Professional) i

3.7.3 EC-Council

- CEH
- CNDA
- ECSA

3.7.4 SANS GIAC

- GISF
- GSEC
- GCIA
- GCIH
- GCUX
- GCWN
- GCED
- GPEN
- GWAPT
- GAWN
- GICSP
- G7799
- GSNA
- GISP
- GSLC
- GCPM
- GSSP-JAVA
- GSSP-.NET
- GWEB
- GCFE
- GCFA
- GREM
- GNFA
- GLEG
- GSE

3.7.5 CompTIA

- Security+ (S+)
- CySA+ (CSA+)
- CASP
- PenTest+

3.7.6 Offensive Security

- OSCP

3.7.7 Cisco Systems

- CCNA Security

- CCNP Security
- CCIE Security

4. Plan de prevención y concienciación.

"Si no puedes ser fuerte, pero tampoco sabes ser débil, serás derrotado." El Arte de la Guerra Sun Tzu

El creciente uso de las nuevas tecnologías en las empresas hace indispensable la concienciación sobre los riesgos asociados a las mismas.

Es necesario que los empleados conozcan y apliquen buenas prácticas en el uso de todo tipo de dispositivos y soluciones tecnológicas para lo cual debemos proporcionarles formación en ciberseguridad adecuada a su puesto ya que de este modo se pueden prevenir la mayoría de los incidentes.

Complej.	Alcance	Control	SI/NO
Básica	Dirección o personal de gestión	Difusión de la política de seguridad	
Básica	Dirección o personal de gestión	Concretar el plan de formación	
Básica	Dirección o personal de gestión	Programas de formación específicos	
Básica	Dirección o personal de gestión	Periodicidad de la formación	
Básica	Dirección o personal de gestión	Evaluación del aprendizaje	
Básica	Dirección o personal de gestión	Promover una cultura de seguridad de la información	

4.0.1 Kit de concienciación del INCIBE
4.1 Prevención
4.1.1 Protección y destrucción de datos
4.1.2 Phishing
Correos electrónicos maliciosos
Phishing de entrada de datos
Phishing móvil
Spear phishig
4.1.3 Protección del correo electrónico
4.1.4 Enlaces peligrosos
4.1.5 Adjuntos peligrosos
4.1.6 Ingeniería social
4.1.7 Amenazas en la rutina diaria
Amenazas a los ejecutivos
Seguridad en dispositivos móviles
Seguridad fuera de la oficina
Redes sociales seguras
Seguridad cuando salimos de viaje
Seguridad USB
4.2 Compliance (cumplimiento normativo)
4.2.1 Reglamento General de Protección de Datos (GDPR)
4.2.2 PCI DSS Información sanitaria protegida
4.2.3 Protección contra el ransomware

5. Taxonomía de los incidentes de ciberseguridad

Cuando ocurre un incidente, para poder clasificarlo, es necesario disponer de una taxonomía de incidentes. Intuitivamente cualquier SysAdmin (administrador de sistemas) o DevOps (encargado de la entrega de aplicaciones y servicios) podría proponer al menos los siguientes:

- **Contenido abusivo**: incidentes que muestren signos evidentes de spam, comentarios ofensivos o inciten a la pederastia, bullying, grooming, goossip, sexting, ciberacoso, violencia y/o delitos sexuales.
- **Fraude**: reportes que tengan nexo con el uso no autorizado, derechos de autor, suplantación de identidad, phishing y robo de credenciales.
- **Contenido malicioso**: problemas relacionados con todo tipo de malware, como virus, troyanos, gusanos, spyware, bots e inyección de código.
- **Recolección de información**: los escaneos como reporte más común. También se consideran dentro de esta clasificación aquellos relacionados con los usos de sniffers, ingeniería social o ataques de fuerza bruta.
- **Acceso/Intrusión**: incidentes en los que se manifieste el claro acceso a cuentas privilegiadas, no privilegiadas, compromiso de aplicaciones y ataques de 0-day.
- **Disponibilidad**: ataques de denegación de servicio, tales como DoS, DDoS y sabotajes.
- **Seguridad/Confidencialidad** de la información: problemas relacionados con el acceso a información y/o modificación no autorizada.

Pero no nos asustemos, no necesitamos crear desde cero nuestra taxonomía, de hecho para Europa, ENISA (la Agencia de la Unión Europea para la Ciberseguridad) propone la siguiente (conviene consultar en su repositorio pues está en contínua evolución):

CLASSIFICATION	EXAMPLES	Description / Examples
Abusive Content	Spam	Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content. This IOC refers to resources which make up spam infrastructure, for example, harvesters like address verification, URLs in spam emails, etc.
Abusive Content	Harmful Speech	Bullying, harassment or discrimination of somebody, e.g., cyber stalking, racism or threats against one or more individuals.
Abusive Content	(Child) Sexual Exploitation/Sexual/Violent Content	Child Sexual Exploitation (CSE), sexual content, glorification of violence, etc.
Malicious Code	Infected System	System infected with malware, e.g., a PC, smartphone or server infected with a rootkit. Most often this refers to a connection to a sinkholed command and control server.
Malicious Code	C2 Server	Command and control server contacted by malware on infected systems.
Malicious Code	Malware Distribution	URI used for malware distribution, e.g., a download URL included in fake invoice malware spam or exploit kits (on websites).
Malicious Code	Malware Configuration	URI hosting a malware configuration file, e.g., web injects for a banking trojan.
Information Gathering	Scanning	Attacks that send requests to a system to discover weaknesses. This also includes testing processes to gather information on hosts, services and accounts. This includes fingerd, DNS querying, ICMP, SMTP (EXPN, RCPT, etc) port scanning.
Information Gathering	Sniffing	Observing and recording of network traffic (i.e. wiretapping).
Information Gathering	Social Engineering	Gathering information from a human being in a non-technical way (e.g., using lies, tricks, bribes, or threats).
Intrusion Attempts	Exploitation of Known Vulnerabilities	An attempt to compromise a system or to disrupt any service by exploiting vulnerabilities with a standardised identifier such as CVE name (e.g., using a buffer overflow, backdoor, cross site scripting)
Intrusion Attempts	Login Attempts	Multiple brute-force login attempts (including guessing or cracking of passwords). This IOC refers to a resource, which has been observed to perform brute-force attacks over a given application protocol.
Intrusion Attempts	New Attack Signature	An attack using an unknown exploit.

CLASSIFICATION	EXAMPLES	Description / Examples
Intrusions	Privileged Account Compromise	Compromise of a system where the attacker has gained administrative privileges.
Intrusions	Unprivileged Account Compromise	Compromise of a system using an unprivileged (user/service) account.
Intrusions	Application Compromise	Compromise of an application by exploiting (un)known software vulnerabilities, e.g., SQL injection.
Intrusions	System Compromise	Compromise of a system, e.g., unauthorised logins or commands. This includes attempts to compromise honeypot systems.
Intrusions	Burglary	Physical intrusion, e.g., into a corporate building or data centre.
Availability	Denial of Service	Denial of Service attack, e.g., sending specially crafted requests to a web application which causes the application to crash or slow down.
Availability	Distributed Denial of Service	Distributed Denial of Service attack, e.g., SYN flood or UDP-based reflection/amplification attacks.
Availability	Misconfiguration	Software misconfiguration resulting in service availability issues, e.g., DNS server with outdated DNSSEC Root Zone KSK.
Availability	Sabotage	Physical sabotage, e.g., cutting wires or malicious arson.
Availability	Outage	An outage caused, for example, by air conditioning failure or natural disaster.
Information Content Security	Unauthorised Access to Information	Unauthorised access to information, e.g., by abusing stolen login credentials for a system or application, intercepting traffic or gaining access to physical documents.
Information Content Security	Unauthorised Modification of Information	Unauthorised modification of information, e.g., by an attacker abusing stolen login credentials for a system or application, or ransomware encrypting data. Also includes defacements.
Information Content Security	Data Loss	Loss of data caused by, for example, hard disk failure or physical theft.
Information Content Security	Leak of Confidential Information	Leaked confidential information, e.g., credentials or personal data.
Fraud	Unauthorised Use of Resources	Using resources for unauthorised purposes including profit-making ventures, e.g., the use of email to participate in illegal profit chain letters or pyramid schemes.
Fraud	Copyright	Offering or installing copies of unlicensed commercial software or other copyright protected materials (also known as Warez).

CLASSIFICATION	EXAMPLES	Description / Examples
Fraud	Masquerade	Type of attack in which one entity illegitimately impersonates the identity of another in order to benefit from it.
Fraud	Phishing	Masquerading as another entity in order to persuade the user to reveal private credentials. This IOC most often refers to a URL, which is used to phish user credentials.
Vulnerable	Weak Cryptography	Publicly accessible services offering weak cryptography, e.g., web servers susceptible to POODLE/FREAK attacks.
Vulnerable	DDoS Amplifier	Publicly accessible services that can be abused for conducting DDoS reflection/amplification attacks, e.g., DNS open-resolvers or NTP servers with monlist enabled.
Vulnerable	Potentially Unwanted Accessible Services	Potentially unwanted publicly accessible services, e.g., Telnet, RDP or VNC.
Vulnerable	Information disclosure	Publicly accessible services potentially disclosing sensitive information, e.g., SNMP or Redis.
Vulnerable	Vulnerable System	A system which is vulnerable to certain attacks, e.g., misconfigured client proxy settings (such as WPAD), outdated operating system version, or cross-site scripting vulnerabilities.
Other	Uncategorised	All incidents which don't fit in one of the given categories should be put into this class or the incident is not categorised.
Other	Undetermined	The categorisation of the incident is unknown/undetermined.
Test	Test	Meant for testing.

En el Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información encontramos una referencia a esta misma tabla.

En los casos de peligrosidad o impacto crítico, muy alto y alto hemos de notificar el incidente inmediatamente. En el caso de crítico, hay que hacer una notificación intermedia en 24/48 horas y una notificación final en 20 días. En el caso de niveles muy altos, lla notificación intermedia será a las 72 horas y la final a los 40 días. Estos requisitos no son necesarios en los niveles alto, medio y bajo (en estos dos últimos no es necesaria ni siquiera la comunicación inicial).

5.1 Contenido Abusivo

Dentro de este apartado tenemos ejemplos como:

- **correo electrónico no deseado o SPAM**: El correo no deseado recibido ocupa un tiempo de nuestros trabajadores que conlleva la consecuente pérdida económica. La cosa se complica aún más si consiguen hacerse con la cuenta de uno de nuestros empleados para enviar correo no deseado, pues entonces nuestros servidores podrían entrar en listas negras o de bloqueo.

Normalmente los proveedores de servicios disponen de mecanismos para limitar el número de mensajes enviados en un determinado espacio de tiempo para evitar precisamente esto.

- **comentarios ofensivos**: Comentarios o publicaciones realizadas para minar la imagen de una empresa o persona.
- **violencia o agresiones**: Hablamos aquí de cualquier tipo de contenido (en texto, audio, vídeo imágenes) sobre abusos sexuales, pederastia, bullying, ciberacoso, grooming (acoso y abuso sexual online, asociado normalmente a pederastia), goossip (difusión de rumores, no necesariamente ciertos, para minar la imagen de una persona), sexting (intercambio de fotografías o vídeos de contenido erótico que luego pueden usarse para extorsión), sextorsión (el paso siguiente al sexting) , o cualquier otro tipo de incitación o violencia y/o delitos sexuales.
- **noticias falsas, bulos o HOAX**: En la era de la información y las redes sociales pueden llevar a un peligroso círculo vicioso de desinformación. Según First Draft News se puede a su vez clasificar en:
  1. Satira o parodia: No pretende causar dano o engano.
  2. Contenido enganoso: Se trata del uso enganoso de la informacion para incriminar a alguien o algo.
  3. Contenido impostor: Es el tipo de informacion que suplanta fuentes genuinas.
  4. Contenido fabricado: Contenido nuevo que es predominantemente falso, disenado especialmente para enganar y perjudicar.
  5. Conexion falsa: Cuando los titulares, imagenes o leyendas no confirman el contenido.
  6. Contexto falso: Cuando el contenido genuino se difunde con informacion de contexto falsa.
  7. Contenido manipulado: Cuando informacion o imagenes genuinas se manipulan para enganar.

5.2 Código Malicioso

En este apartado hablamos de:

1. Sistema infectado.
   1. Sistema infectado con malware. Ej.: sistema, computadora o teléfono móvil infectado con un rootkit.
2. Servidor C&C (Mando y Control).
   1. Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
3. Distribución de malware.
   1. Recurso usado para distribución de malware. Ej.: recurso de una organización empleado para distribuir malware.
4. Configuración de malware.
   1. Recurso que aloje ficheros de configuración de malware Ej.: ataque de webinjects para troyano.

5.3 Recolección de información

Hablamos de recolección de información en los siguientes casos:

1. Escaneo de redes (scanning).
   1. Envío de peticiones a un sistema para descubrir posibles debilidades. Se incluyen también procesos de comprobación o testeo para recopilar información de alojamientos,

servicios y cuentas. Ej.: peticiones DNS, ICMP, SMTP, escaneo de puertos.

2. Análisis de paquetes (sniffing).
    1. Observación y grabación del tráfico de redes.
3. Ingeniería social.
    1. Recopilación de información personal sin el uso de la tecnología. Ej.: mentiras, trucos, sobornos, amenazas.

5.4 Intento de intrusiones

Hablamos de intento de intrusión en los siguientes casos:

1. Explotación de vulnerabilidades conocidas.
    1. Intento de compromiso de un sistema o de interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estandarizado (véase CVE). Ej.: desbordamiento de buffer, puertas traseras, cross site scripting (XSS).
2. Intento de acceso con vulneración de credenciales.
    1. Múltiples intentos de vulnerar credenciales. Ej.: intentos de ruptura de contraseñas, ataque por fuerza bruta.
3. Ataque desconocido.
    1. Ataque empleando exploit desconocido.

5.5 Intrusiones

Son intrusiones:

1. Compromiso de cuenta con privilegios.
    1. Compromiso de un sistema en el que el atacante ha adquirido privilegios.
    2. Compromiso de cuenta sin privilegios.
    3. Compromiso de un sistema empleando cuentas sin privilegios.
2. Compromiso de aplicaciones.
    1. Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ej.: inyección SQL.
3. Robo.
    1. Intrusión física. Ej.: acceso no autorizado a Centro de Proceso de Datos.

5.6 Disponibilidad

Incidentes que afecten a la disponibilidad son:

1. DoS (Denegación de servicio): Ataque de denegación de servicio. Ej.: envío de peticiones a una aplicación web que provoca la interrupción o ralentización en la prestación del servicio.
2. DDoS (Denegación distribuida de servicio): Ataque de denegación distribuida de servicio. Ej.: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
3. Mala configuración: Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej.: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
4. Sabotaje. Sabotaje físico. Ej.: cortes de cableados de equipos o incendios provocados.
5. Interrupciones. Interrupciones por causas ajenas. Ej.: desastre natural.

5.7 Seguridad y confidencialidad de la información

Incidentes sobre la seguridad y confidencialidad de la información son:

1. Acceso no autorizado a información. Ej.: robo de credenciales de acceso mediante interceptación de tráfico o mediante el acceso a documentos físicos.
2. Modificación no autorizada de información. Ej.: modificación por un atacante empleando credenciales sustraídas de un sistema o aplicación o encriptado de datos mediante ransomware.
3. Pérdida de datos. Pérdida de información Ej.: pérdida por fallo de disco duro o robo físico.

5.8 Fraude

Casos de fraude pueden ser:

1. Uso no autorizado de recursos. Uso de recursos para propósitos inadecuados, incluyendo acciones con ánimo de lucro. Ej.: uso de correo electrónico para participar en estafas piramidales.
2. Derechos de autor. Ofrecimiento o instalación de software carente de licencia u otro material protegido por derechos de autor. Ej.: Warez.
3. Suplantación: Tipo de ataque en el que una entidad suplanta a otra para obtener beneficios ilegítimos.
4. Phishing: Suplantación de otra entidad con la finalidad de convencer al usuario para que revele sus credenciales privadas.

5.9 Vulnerabilidades

Ejemplos de vulnerabilidades:

1. Criptografía débil. Servicios accesibles públicamente que puedan presentar criptografía débil. Ej.: servidores web susceptibles de ataques POODLE/FREAK.
2. Amplificador DDoS. Servicios accesibles públicamente que puedan ser empleados para la reflexión o amplificación de ataques DDoS. Ej.: DNS open-resolvers o Servidores NTP con monitorización monlist.
3. Servicios con acceso potencial no deseado. Ej.: Telnet, RDP o VNC.
4. Revelación de información. Acceso público a servicios en los que potencialmente pueda relevarse información sensible. Ej.: SNMP o Redis.
5. Sistema vulnerable. Ej.: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.

5.10 Otros

Todo aquel incidente que no tenga cabida en ninguna categoría anterior. Aquí también podemos englogar las APT: Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos o genuinos.

5.11 Bibliografía para ampliar

- Reference Incident Classification Taxonomy, ENISA, Enero 2018
- Common Taxonomy for Law Enforcement and CSIRTs, EUROPOL, Diciembre de 2021
- REFERENCE TAXONOMY INCIDENT Taxonomy (human readable version)

III Tercera Parte

6 OSINT 67
6.1 Recopilación de datos
6.2 Metodología
6.3 Casos prácticos
6.4 LinuxMint OSINT
6.5 Herramientas on-line

6. OSINT

Llamamos Inteligencia de fuentes abiertas u «Open Source Intelligence» (OSINT) al conocimiento recopilado a partir de fuentes de acceso público, ojo público no quiere decir gratuito, también es posible *"comprar"* esa información de manera **lícita**. El proceso incluye la búsqueda, selección y adquisición de la información, así como un posterior procesado y análisis de la misma con el fin de obtener conocimiento útil y aplicable en distintos ámbitos.

OSINT es una de las disciplinas de recolección de inteligencia, como también lo son:

1. HUMINT: Hace referencia a la inteligencia recogida a partir de una persona en un espacio en cuestión.
2. GEOINT: Inteligencia geoespacial.
3. IMINT: Inteligencia a partir de imágenes.
4. MASINT: Inteligencia de medidas de señales, como pueden ser: nucleares, electromagnéticas, ópticas, de radar, radiofrecuencia, materiales (a partir de estudios químicos, análisis nucleares...).
5. SIGINT: Inteligencia obtenida a partir de la interceptación de señales.
6. TECHINT: Inteligencia obtenida a partir del estudio de la tecnología de países o empresas externas.
7. CYBINT/DNINT: Inteligencia cibernética o digital.
8. FININT: Inteligencia financiera.

Existen multitud de fuentes abiertas a partir de las cuales se puede obtener información relevante, entre las que destacan:

- Medios de comunicación: revistas, periódicos, radio, etc.
- Información pública de fuentes gubernamentales.
- Foros, redes sociales, blogs, wikis, etc.
- Conferencias, simposios, «papers», bibliotecas online, etc.

Algunos ejemplos de la utilización de OSINT son los siguientes:

- Conocer la reputación online de un usuario o empresa.
- Realizar estudios sociológicos, psicológicos, lingüísticos, etc.

- Auditoria de empresas y diferentes organismos con el fin de evaluar el nivel de privacidad y seguridad.
- Evaluar tendencias de mercados.
- Identificación y prevención de posibles amenazas en el ámbito militar o de la seguridad nacional.
- Como aspecto negativo, es utilizado por cibercriminales para lanzar ataques APT y «Spear Phishing».

El proceso OSINT consta de las siguientes fases:

1. Dirección y planificación: es la fase en la que se establecen todos los requerimientos que se deben cumplir, es decir, aquellas condiciones que deben satisfacerse para conseguir el objetivo o resolver el problema que ha originado el desarrollo del sistema OSINT.
2. Adquisición: consiste en especificar, a partir de los requisitos establecidos, las fuentes de interés que serán recopiladas. Hay que tener presente que el volumen de información disponible en Internet es prácticamente inabordable por lo que se deben identificar y concretar las fuentes de información relevante con el fin de optimizar el proceso de adquisición.
3. Procesamiento: etapa en la que se obtiene la información a partir de los orígenes indicados y se da formato a toda la información recopilada de manera que posteriormente pueda ser analizada.
4. Análisis e integración: es la fase en la que se genera inteligencia a partir de los datos recopilados y procesados. El objetivo es relacionar la información de distintos orígenes buscando patrones que permitan llegar a alguna conclusión significativa.
5. Difusión y feedback: consiste en presentar la información obtenida de una manera eficaz, potencialmente útil y comprensible, de manera que pueda ser correctamente explotada.

Se pueden identificar principalmente 2 problemas a la hora de utilizar un sistema OSINT:

- Demasiada información: como ya se ha puesto de manifiesto, la cantidad de información pública disponible en Internet es más que notable. Es por ello, que se debe realizar un proceso muy exhaustivo a la hora de identificar y seleccionar las fuentes de información de interés que van a ser recopiladas, y que posteriormente servirán para la generación de inteligencia. El hecho de utilizar un catálogo extenso de fuentes conlleva obviamente un mayor gasto a la hora de implementar el sistema, y en el caso de no tener disponibles los recursos necesarios, provoca una significativa ralentización del mismo.
- Fiabilidad de las fuentes: es importante valorar previamente las fuentes que van a nutrir el sistema de información ya que una selección errónea de las mismas puede provocar resultados erróneos y desinformación.

6.1 Recopilación de datos

Aunque hoy día existen plataformas o sistemas como Maltego o Leonardo que combinan herramientas de Big Data e Inteligencia Artificial para ayudar a comprender y seguir el rastro de la información de nuestras investigaciones, normalmente el investigador OSINT usa diferentes herramientas Web combinadas con otros script (normalmente en Python) de elaboración propia o específicos para el tipo de investigación.

A la hora de hacer una investigación, es clave la clasificación y registro de la información, es decir, qué información, cuando, de dónde y cómo fue extraida cada pieza de información así como si los datos han sido tratados o no y por supuesto, hay que almacenar como evidencia siempre una copia del original sin manipular (para ello es importante usar algoritmos de huella digital).

La red es un medio voluble, es decir, cambiante, que no podemos controlar, por ello es

Figura 6.1: Fases OSINT

importante dejar registrado:

1. La fuente de procedencia del documento. La falta de control y confiabilidad de los contenidos de la red así como la cantidad ingente de información (infoxicación) nos obliga a tener en cuenta si es veraz y cierta la información o no; podríamos estar ante una "fake new"...
2. Atribución: Quién se responsabiliza de la información publicada.
3. Temporalidad: En determinados ámbitos la información tiene una temprana fecha de caducidad.

Dicho esto, podemos establecer una escala de valoración de fuentes basada en dos coordenadas en base a estas dos tablas.

Tabla 1: Valoración de la fuente:

valor	valoración de la fuente
1	Fuente bien conocida y que lleva tiempo proporcionando info válida
2	Fuente bien conocida y con larga trayectoria pero que a veces ha proporcionado que con el tiempo se ha comprobado errónea o falsa
3	Fuente fiable pero joven, con poca trayectoria
4	Fuente dudosa que lleva tiempo proporcionando informaciones de escasa fiabilidad
5	Fuente desconocida sin referencias

Tabla 2: Valoración de la información:

valor	valoración de la información
A	Información creible
B	FInformación que corresponde con hechos previos pero en la que hay flecos que debemos investigar
C	Información que contradice tenddencias y hechos previos bien conocidos, puede ser incorrecta y por tanto conviene investigar
D	La información choca con tendencias y hechos conocidos. Es altamente dudosa
E	La información puede ser creíble, pero no hay manera de comprarla con informaciones previas

Tal y como jugamos al conocido juego de los barcos, con estas dos coordenadas damos una valoración de la fuente y la información para nuestro informe.

6.2 Metodología

Conceptos previos:

- **Entidad**: Algo único, como una persona por el ID de su cuenta en redes sociales o un vehículo por el VIN o número de bastidor.
- **Tiempo**: Como una sucesión de acontecimientos contínua.
- **Espacio**: Lugar donde sucede un hecho o el objetivo se mueve.
- **Suceso**: Implica a varias entidades y se concreta en el espacio y el tiempo. Si no ha tenido lugar o **no podemos demostrar su realidad**[1], no es un suceso.
- **Relación**: nexos entre entidades, entidades y tiempo, entidades y sucesos...

[1] Por esta razón es tan importante almacenar en un SIEM una copia de todos los eventos de nuestros sistemas. Si no tenemos constancia de un ataque, fuga, sabotaje... no podemos estudiar qué ocurrió, no hubo suceso.

6.2.1 Modos de recopilación de información

En la fase de recopilación de datos, según la investigación, tendremos varias maneras de objener la información:

- Recopilación pasiva: usando una herramienta y sin conimiento de las entidades o personas afectadas.
- Recopilación activa: Cuando no hay información en abierto y tenemos que *acercarnos* un poco al objetivo para obtener información.
- Ingeniería social: Cuando no ha nada de información en abierto y no es posible acercarnos de manera sigilosa al objetivo.

6.2.2 El entorno de trabajo

Nuestra vida digital deja un rastro o huella inherente a cualquier actividad (búsquedas, compras, correo, redes sociales...) es por ell que el primer paso como *investigador de inteligencia* es separar totalmente la vida personal de la profesional.

Cualquier exposición de nuestros datos personales puede poner en riesgo una investigación por lo que es recomendable tener una identidad totalmente distinta para el entorno laboral y además seguir los pasos básicos de seguridad:

1. Usar siempre contraseñas diferentes en todos los sitios Web y aplicaciones que usemos. Esta tarea, aunque complicada, puede simplificarse considerablemente usando un gestor de contraseñas como KeeePassXC que además tiene integración nativa con la mayoría de los navegadores, es multiplataforma y permite exportar el almacén de contraseñas, que por supuesto, está cifrado con AES-256.
2. Usar siempre autenticación de doble factor (2FA, algo que tengo y algo que sé...) para acceder a las cuentas y/o servicios online (email, nuestra propia VPN, la VPN contratada para fuera de la oficina, etc.).
3. No abrir emails de remitentes desconocidos. Mediante javascript (normalmente) es posible entrar en sistemas vulnerables, robando credenciales (recuerda que muchos servicios funcionan en base a tokens, una vez nos autenticamos en el sistema, para las siguientes peticiones o comunicaciones, usamos el token en vez de volver a autenticar; si nos roban el token, pueden suplantarnos).
4. Evitar la geolocalización en aplicaciones, mensajes, redes sociales...
5. Hacer **Egosurfing** de vez en cuando, es decir, buscarnos en la red para ver qué información hay de nosotros o si alguien intenta suplantarnos.
6. Usar entornos virtualizados (máquinas virtuales) para nuestras investigaciones
7. Usar anonimizadores de la conexión como servicios de pago de VPN o la red gratuita TOR. Si se trata de una investigación extremadamente secreta, podemos usar sistemas operativos como Tails.
8. Usar software original y legítimo siempre.
9. Crear identidades nuevas para cada investigación para no "quemar" las que usamos con regularidad.
10. No navegar con la pantalla maximizada (para evitar que puedan adivinar el hardware que tenemos).

En cuanto a la información sensible, recuerda siempre tenerla cifrada, ya sea desde el sistema operativo o, si el sistema lo permite, mediante hardware. Siempre que activemos el cifrado de datos del disco del sistema, el rendimiento se ve afectado, incluso cuando el procesador tenga extensiones AES-NI precisamente para acelerar este tipo de operaciones. Para activar que todo el sistema esté cifado podemos hacerlo con:

1. Cifrado de disco en Linux: LUKS. La gran mayoría de las distribuciones Linux permiten en tiempo de instalación que la partición principal del sistema operativo esté cifrada. De esta manera protegemos al sistema de manipulaciones y/o alteraciones mientras esté apagado. Podemos encontrar problemas si usamos LVM (Logical Volume Manager) para añadir espacio a las particiones sin formatear, por ejemplo:
    1. LUKS sobre una partición: La configuración básica y más sencilla sin LVM, la partición está cifrada.
    2. LUKS sobre LVM: Los volúmenes requieren claves propias cada uno, habría que usar **dm-crypt**. El esquema LVM es transparente cuando está bloqueado. LVM puede utilizarse para tener cifrado volúmenes que abarquen varios discos. Facilidad para mezclar grupos de volúmenes cifrados/descifrados
    3. LVM dentro de una única partición LUKS. Solo es necesaria una clave para desbloquear todos los volúmenes. Es el mejor esquema para tareas como suspensión del disco (piensa en un portátil, por ejemplo, que pida la clave cada vez que cierras la tapa y se hiberna)
2. Cifrado de disco en Mac: FileVault. En los ajustes de seguridad de MacOS podemos activa el cifrado de discos para Machintosh. Se puede hacer en caliente y sobre una partición no cifrada y viceversa, una partición cifrada puede descifrarse. Permite crear archivos de imagen y cifrar la imagen en lectura/escritura.
3. Cifrado de disco en Windows: BitLocker. Desde el *panel de control*, en *sistema y seguridad*, tenemos la opción *cifrado de unidad BitLocker*.

6.3 Casos prácticos

6.3.1 Modelo de actuación para casos de phising

La empresa Acme Inc. contrata nuestros servicios para analizar un ataque de phising que han sufrido sus empleados y clientes. Ejemplo de procedimiento:

1. Análisis cualitativo de cabeceras, es decir, analizar todo el contenido y logos para ver posibles suplantaciones de identidad o robo de credenciales. Para encaminar la investigación desde el atacante.
2. Utilizar recursos como The harvester o Maltego para ver relaciones. Así como una herramienta muy buena denominada Darktracer para ver posibles relaciones con grupos de ransomware.
3. Cotejar las URL con herramientas como Fofa, Shodan o Foca, para un análisis más profundo. También cotejar las IP con virustotal o Shodan así como utilizar Nmap para recopilar más datos.
4. Cotejar las IOCs (Indicators Of Compromise) con casos anteriores publicados por investigadores o los CERT de referencia nacionales o internacionales. Así como los análisis de malware propios de personas en redes como github, Twitter o foros de hackers conocidos.
5. Si afecta a infraestructuras críticas, comunicar a INCIBER CERT para ayudar a la protección de infraestructuras críticas (en el caso de España).
6. En el caso de que sean SMS, cotejar con la CNMC con la operadora y alertarla de que se está produciendo phishing desde un número de teléfono dado de alta en sus líneas.

6.4 LinuxMint OSINT

Receta para crear una máquina para investigación OSINT.
Descargamos ISO de LinuxMint y con shasum -a 256 comprobamos la integridad de la imagen.
Actualizamos el sistema:

```
sudo apt update
sudo apt upgrade
sudo apt install kate git vim python3-pip
```

6.4.1 Herramientas para Youtube

Herramientas OSINT para Youtube:

```
sudo apt install youtube-dl
pip3 install yt-dlp
```

IMPORTANTE: Python instala sus *ejecutables* en la ruta *$HOME/.local/bin*, luego tenemos que añadir esta ruta a nuestra variable PATH.

1. Usamos youtube-dl para descargas normales
2. Usamos yt-dlp para descargas complejas como vídeos fragmentados, usando para ello la lista de vídeos (fichero m3u8)

Para automatizar esta tarea, podemos crearnos un script bash:

```
#!/bin/bash

DIR=$HOME/OSINT
VIDEO_DIR="$DIR/Youtube"
marcatiempo=$(date +%Y-%m-%d-%H:%M:%S)

if [[ ! -d $DIR ]]
then
    echo "No exist a el directorio $DIR, creado"
    mkdir $DIR
fi

if [[ ! -d $VIDEO_DIR ]]
then
    echo "No exist a el directorio $VIDEO_DIR, creado"
    mkdir $VIDEO_DIR
fi

url=$(zenity --entry --title "Descarga de Youtube" --text "URL:")
yt-dlp "$url" -o "$VIDEO_DIR/$marcatiempo%(title)s.%(ext)s" \
 --all-subs -i | zenity --progress --pulsate --no-cancel --auto-close \
 --title "Descargando v deo..."
```

Ahora faltaría darle permisos de ejecución al archivo con:

```
chmod +x youtube.sh
```

6.4.2 Herramientas para Instagram

Para esta red social tenemos herramientas tan interesantes como:

- instaloader
- instalooter
- toutatis

- Osintgram

```
cd
cd OSINT
git clone https://github.com/Datalux/Osintgram
cd Osintgram
pip3 install -r requirements.txt
python3 main.py -c photos elmonaguillo
python3 main.py -c fwersemail elmonaguillo
```

Para aprender más sobre Osintgram, en este vídeo nos dan más pistas.

6.4.3 Herramientas de usuario / correo electrónico

Existen multitud de herramientas como:

1. Sherlock
2. Holene
3. SocialScan
4. WhatsMyName
5. Email2Phone

Instalación de **Sherlock**:

```
# clone the repo
$ git clone https://github.com/sherlock-project/sherlock.git

# change the working directory to sherlock
$ cd sherlock

# install the requirements
$ python3 -m pip install -r requirements.txt
```

Instalación y uso de **Holehe**:

```
pip3 install holehe
holehe juan@sincorreo.com
```

6.4.4 Herramientas para analizar redes (CLI)

1. amass: Busca subdominios dentro del indicado.
2. TheHarvester:
3. Photon
4. Carbon14
5. EyeWhitness
6. Rastrea2r

```
docker pull caffix/amass
docker run -v OUTPUT_DIR_PATH:/.config/amass/ caffix/amass enum -share -d iesv
```

6.4.5 Herramientas para investigar redes (Web)

- WiFi: Wigle: Permite buscar por SSID, BSSID, área, etc.

- Por IP: Shodan: La cuenta gratuita permite 100 búsquedas al mes. Nos permite ver puertos abiertos sin hacer escaneo activo. También se puede hacer consultas sencillas sin login así: http://https://beta.shodan.io/host/88.26.231.151 -en este momento esta es la IP del IES-.
- Reverse DNS: ViewDNS, ejemplo: `https://viewdns.info/reverseip/?host=2.139.173.60`
- Geolocalización: iplocation.net. Consulta varios servicios de geolocalización. Si lo probamos con la IP del centro, no termina de llegar con precisión a nuestra localización, pero se acerca bastante: `https://www.iplocation.net/ip-lookup?query=88.26.231.151&submitIP+Lookup`.

Por supuesto que no podemos dejar este apartado de búsqueda avanzada sin hablar del gigante de las búsquedas: Google. Todos probablemente conocemos estos comandos avanzados de búsqueda de Google:

- "término de búsqueda" Utiliza este para hacer una búsqueda exacta.
- OR busca esto o aquello. Este devolverá resultados relacionados con los dos términos o con ambos.
- AND buscar esto y aquello. Este solo devolverá resultados relacionados con los dos términos
- – Excluir un término o una frase de búsqueda.
- * Actúa como un comodín y encontrará cualquier palabra o frase.
- ( ) Agrupa múltiples términos u operadores para controlar cómo se muestra la búsqueda.
- $ Busca los precios.
- define: Muestra el significado de una palabra en un resultado similar a una tarjeta.
- Cache: Devuelve la versión en caché más reciente de una página web (siempre que la página esté indexada).
- filetype: Muestra los resultados de un determinado tipo de archivo (PDF, DOCX, TXT, PPT, etc.)
- site: Limita los resultados a un sitio web específico.
- related: Encuentra sitios relacionados con otro sitio.
- intitle: Encuentra las páginas que contienen una palabra específica en el título.
- allintitle: Similar a «intitle», este encuentra páginas web que contienen todas las palabras específicas del título de la página.
- inurl: Encuentra páginas con una determinada palabra en la URL.
- allinurl: Similar a «inurl», este encuentra páginas web que contienen todas las palabras específicas en el URL.
- intext: Encuentra las páginas que contienen una palabra específica en el contenido
- allintext: Encuentra resultados que contienen todas las palabras específicas en algún lugar de la página.
- AROUND(X) Esta búsqueda por proximidad encuentra páginas que contienen dos palabras (o frases) dentro de X palabras entre sí.
- weather: Encuentra el tiempo para un lugar específico.
- stocks: Muestra información sobre las acciones
- map: Muestra los resultados del mapa para una búsqueda de ubicación.
- movie: Encuentra información sobre una película específica.
- in: Convertir una unidad en otra (como monedas, pesos, temperaturas, etc.)
- source: Encuentra resultados de noticias de una cierta fuente en Google News.

Ahora viene la parte interesante, que es conocido en el argot como Google Dorks, que es combinar este conocimiento para llegar a información sensible, sitios vulnerables, etc. Veamos unos ejemplos:

- **intitle:index.of “Apache/*” “server at” site:.es**: Esto busca servidores Apache que muestran la versión en España. Vamos a encontrar muchos organismos públicos y Universidades.
- **intitle:“toshiba network camera – User Login”**: Da acceso a muchos grabadores o NVR abiertos a Internet.
- **“teléfono * * *dirección* ” “e-mail” intitle:“curriculum vitae”**: Información personal sesible de muchas personas que tienen su CV expuesto en Internet.

6.4.6 Herramientas de Telegram

- Fuente: Awesome Telegram OSINT

6.4.7 Herramientas de Office 365

- PWC - Office365 Extractor

6.4.8 Herramientas búsqueda de código

- Grep.APP
- SourceGraph

6.4.9 Herramientas para investigar Proton Mail y VPN

- ProtOSINT

6.5 Herramientas on-line

6.5.1 Webs para buscar archivos en servidores FTP

- Archie
- Global file search
- Mamont
- NAPALM FTP Indexer

6.5.2 Webs para ampliar conocimientos sobre OSINT

Además de los numerosos canales de Telegram y Discord tanto de la comunidad latina como internacional, os proponemos unos enlaces donde encontrar más información:

- OSINT Resources Portal
- Intelligence Techniques
- Brigada OSINT
- Ciberpatrulla - Herramientas OSINT
- The Book of Secret Knoledge
- Nix Intelligence
- We’re OSINTCurious.us

IV

Cuarta Parte

7 Preparación. Configuraciones seguras. MITRE 79
7.1 ¿Y si sucede un incidente?
7.2 Mecanismos de defensa
7.3 Mitre ATT&CK

8 Detección de incidentes 93
8.1 IDS
8.2 SOC
8.3 SIEM

9 Respuesta ante incidentes 95
9.1 Contención
9.2 Erradicación
9.3 Recuperación

10 Actividad postincidente 97
10.1 Documentación, evidencias y ciclo de mejora

7. Preparación. Configuraciones seguras. MITRE

Este tema se centra en la implantación de los **mecanismos de defensa** o conjunto de las capacidades y medidas para prevenir, detectar, reaccionar y recuperar la infraestructura TIC de ataques, intrusiones, interrupciones o acciones hostiles.

El objetivo de estos mecanismos es proteger la integridad, confidencialidad y disponibilidad de la información así como los sistemas que la manejan.

Como ya hemos visto con anterioridad, para poder asegurar el entorno y empezar a trabajar en herrameintas que nos ayuden a detectar y migitigar posibles incidentes, previamente hemos de tener una *casa ordenada*, para ello recordamos lo básico una vez más:

- Credenciales: son las llaves del reino. Hoy día usamos usuarios y contraseñas para prácticamente cualquier actividad relacionada con la tecnología. Debemos de seguir una buena política de contraseñas y además reforzarla con 2FA (autenticación de doble factor). También hay que tener en cuenta que muchas aplicaciones, una vez autenticados, proporcionan un token para evitar tener que autenticarnos en cada interacción. Estos tókenes (cookies de sesión, JWT, etc.) tienen la misma valía que nuestros datos de acceso, pues son equivalentes.
- Bastionado de redes y servicios. Implantación de firewalls, segmentación de redes, securización de la DMZ...
- Las VPNs son nuestra amigas: Para evitar dar la más mínima información al adversario (tráfico DNS, direcciones IP a las que conectamos...) deberíamos usar VPNs siempre que sea posible.
- Sin registros no hay incidente. Hay que implementar un servicio remoto de recogida de eventos para evitar su manipulación cuando uno de nuestros servicios, equipos o redes sean comprometidos. Como ya vimos en capítulos anteriores, es lo que llamamos SIEM (Security Information and Event Management).
- Antivirus y software: actualizados en todos y cada uno de los equipos conectados a la red corporativa.
- Todo el software siempre legal y comprado/descargado de la fuente original oficial.
- Formación y concienciación de los empleados.

7.1 ¿Y si sucede un incidente?

Antes que suceda, todo el mundo debe saber cómo actuar en caso de incidente, para ello, como ya vimos en el tema de normativa, políticas y auditorías, la empresa debe tener una política de ciberseguridad donde todo el mundo tenga claras las guías y medidas de seguridad.

Aún así, por muy buenas que sean nuestras guías, eventualmente ocurrirá un incidente, en cuyo caso todo el personal de la empresa debe conocer el método (plataforma de tickets, correo, etc.) para hacerlo llegar al equipo de respuesta de incidentes de la empresa (CSIRT).

Una vez nos llega al equipo de respuesta, como escalamos incidentes al CSIRT de referencia (Equipo de Respuesta ante Emergencias Informáticas gubernamental) depende mucho de la estructura de nuestra organización. Normalmente en una gran empresa podemos encontrar uno de estos tres modelos:

- SOC
  - En este modelo el SOC es el responsable de la respuesta ante incidentes, ya sea un equipo dentro de la compañía o bien por un servicio contratado externo, lo que se conoce como Managed Security Service Provider (MSSP).
  - Desde la notificación hasta la escalada, los pasos a seguir serían:
    1. La alerta es recibida pon un analista de nivel 1.
    2. Dicho analista estudia si cumple los requisitos para declararlo incidente de ciberseguridad.
    3. Cuando se identifica un potencial incidente, se procede a llevar a cabo una investigación inicial.
    4. Si está justificado, el analista escala el incidente al SOC Manager.
    5. Después de ser revisado, el incidente es escalado al gestor del CSIRT para gestionar el incidente.
  - En este modelo, hay una serie de preocupaciones que deben ser resueltas por el personal del SOC y del CSIRT:
    1. Al CSIRT llegan incidentes antes de estar totalmente envuelto y tener todo el control e información.
    2. Si no se documenta bien la comunicación del incidente, el gestor del CSIRT tendrá que volver atrás y pedir más datos al gestor del SOC, perdiendo un tiempo que puede ser crucial para la resolución del incidente.
    3. El personal del SOC va a necesitar adiestramiento para determinar qué eventos constituyen un incidente y cuáles serán falsos positivos, en caso contrario al CSIRT puede quemarse de cazar los falsos positivos lanzados por el SOC.
    4. La comunicación entre el SOC y el CSIRT debe ser clara y concisa. Cualquier brecha de comunicación al compartir información entre ellos, causará confusión adicional.
- SOC + CSIRT
  - Para evitar algunos de los inconvenientes del modelo de escalada de incidentes SOC, algunas organizaciones integran el SOC dentro del equipo CSIRT. La labor del SOC es entonces alerta inicial y triaje.
  - En este modelo el analista SOC sirve en el primer nivel. Son los que reciben los eventos y alertas de seguridad. Tras procesarlos y el triaje, tienen la posibilidad de escalar el incidente a los analistas de nivel 2, sin necesidad de involucrar a ningún manager del SOC para que lo escale al manager del CSIRT.
  - Este modelo es idóneo para organizaciones que tienen su propio SOC. Para compañías que hace uso de un NOC (Network Operation Center) o un helpdesk sin un SOC

dedicado, es imposible porque estas operaciones se gestionan fuera del CSIRT o, incluso, fuera de los equipos de seguridad de redes.
    - Una ventaja de este modelo es que la escalada y respuesta a incidentes es mucho más rápida y, probablemente, más precisa.
- CFC CSIRT (Cyber Fusion Center Computer Security Incident Response Team)
    - Los CFC son considerados el futuro de los SOC. La principal diferencia es la integración de la inteligencia de amenazas (threat intelligence) en las operaciones de seguridad, dando lugar así a los CSIRT Fusion Center o CFC CSIRT.
    - Combinamos elementos del SOC y CSIRT para dar lugar a un equipo de análisis en inteligencia de ciberamenazas (threat intelligence analyst). Los analistas de amenazas son responsables de enriquecer las investigaciones de incidentes con recursos internos y externos relaciones con los mismos. También pueden tener en cuenta otras áreas relacionadas con el incidente.

Antes de continuar con los siguientes pasos a seguir en el caso de incidente queremos recalcar que todas estas comunicaciones de manera vertical probablemente usarán una plataforma específica o al menos el correo electrónico interno de la empresa, pero para discusión y comunicación horizontal, los equipos necesitan de un espacio donde discutir y llegar a conclusiones, hablamos de la *sala de guerra* o **war room**.

7.1.1 Comunicación del incidente

De manera general, y como vimos en temas anteriores, ya deberíamos de tener dispuesto un plan de contingencias para saber cómo actuar según el tipo de incidente.

De forma particular, el Sector Público, los ciudadanos y empresas, las infraestructuras críticas y operadores estratégicos, las redes académicas y de investigación, así como las redes de defensa de España, tienen a su disposición una serie de organismos de referencia, en los cuales se fundamenta la capacidad de respuesta a incidentes de ciberseguridad (CSIRT) del Gobierno de España:

- CCN-CERT, del Centro Criptológico Nacional del Centro Nacional de Inteligencia, con un ámbito competencial en el Sector Público general, autonómico y local, y sistemas que manejan información clasificada.
- INCIBE-CERT, del Instituto Nacional de Ciberseguridad de España, con un ámbito competencial en la ciudadanía y el sector privado. Asimismo, INCIBE- CERT es el CERT que presta servicios de respuesta a incidentes a las instituciones afiliadas a RedIRIS, la red académica y de investigación española, en coordinación con el CCN-CERT en lo que se refiere a organismos públicos.
- Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), con un ámbito competencial en las infraestructuras críticas y operadores críticos, cuyas capacidades de respuesta técnica se materializan a través de los CSIRT de referencia. Es asimismo autoridad competente para aquellos operadores de servicios esenciales que son además críticos, siendo en ese caso la Oficina de Coordinación Cibernética la responsable de la coordinación en los supuestos previstos en el segundo párrafo del artículo 11.2 del Real Decreto-ley 12/2018.

7.1.2 Sistema de ventanilla única

Según la **GUÍA NACIONAL DE NOTIFICACIÓN Y GESTIÓN DE CIBERINCIDENTES**, en función de la naturaleza del afectado, deberá ser remitida de acuerdo al cauce establecido por su autoridad competente o CSIRT de referencia siguiendo el siguiente esquema:

1. El sujeto afectado enviará un correo electrónico (o ticket) al CSIRT de referencia (INCIBE-CERT o CCN-CERT) notificando el incidente.

2. El CSIRT de referencia, dependiendo del incidente, pone en conocimiento del mismo al organismo receptor implicado o a la autoridad nacional competente.
   - Si afecta a la Defensa Nacional, al CSIRT de referencia ESP-DEF-CERT.
   - Si afecta a una Infraestructura Crítica de la Ley PIC 8/2011, al CNPIC
   - Si afecta al RGPD, a la AEPD.
   - Si es un incidente de AAPP bajo el ENS de peligrosidad ALTA, MUY ALTA o CRÍTICA, al CCN-CERT
   - Si es un incidente de obligado reporte según el RD 12/2018, a la Autoridad Nacional correspondiente:
     - RGPD: se remite a la URL del portal de la AEPD.
     - BDE: se remite la plantilla de notificación .XLS del BDE.
     - PIC: se remite la plantilla de notificación .XLS del CNPIC.
     - ENS: se remite la plantilla de notificación .DOC al CCN-CERT.
     - NIS: se remite la plantilla de notificación de la Autoridad Nacional competente.
3. El Organismo receptor implicado o Autoridad Nacional competente se pone en contacto con el afectado para recabar información:
   1. RGPD: se remite a la URL del portal de la AEPD.
   2. BDE: se remite la plantilla de notificación .XLS del BDE.
   3. PIC: se remite la plantilla de notificación .XLS del CNPIC.
   4. ENS: se remite la plantilla de notificación .DOC al CCN-CERT.
   5. NIS: se remite la plantilla de notificación de la Autoridad Nacional competente.
4. El sujeto afectado comunica los datos necesarios al Organismo receptor implicado o Autoridad Nacional competente.
5. Si procede, desde la Oficina de Coordinación Cibernética (CNPIC), se pone la información a disposición de las Fuerzas y Cuerpos de Seguridad del Estado y Ministerio Fiscal para iniciar la investigación policial y judicial (art. 14.3 RD Ley 12/2018). De acuerdo con el Artículo 11.2 del RD Ley 12/2018, de 7 de septiembre, en los supuestos de especial gravedad que reglamentariamente se determinen y que requieran un nivel de coordinación superior al necesario en situaciones ordinarias, el CCN-CERT ejercerá la coordinación nacional de la respuesta técnica de los CSIRT.

7.1.3 Criterios para la notificación

Para saber si tenemos que notificar un incidente usamos un nivel de peligrosidad aunque también podamos asignarle un nivel de impacto. De esta manera los niveles de peligrosidad serán:

1. Crítico
   1. Un APT (amenaza persistente avanzada)
2. Muy alto
   1. Código dañino
      1. Distribución de malware
      2. Configuración de malware
   2. Intrusión
      1. Robo
   3. Disponibilidad
      1. Sabotaje
      2. Interrupciones
3. Alto
   1. Contenido abusivo

        1. Pornografía infantil, contenido sexual o violento inadecuado
    2. Código dañino
        1. Sistema infectado
        2. Servidor C&C (command and control)
    3. Intrusión
        1. Compromiso de aplicaciones
        2. Compromiso de cuentas con privilegios
    4. Intento de intrusión
    5. Disponibilidad
        1. DoS (denegación de servicio)
        2. DDoS (denegación distribuida de servicio)
    6. Compromiso a la información
        1. Acceso no autorizado
        2. Modificación no autorizada
        3. Pérdida de datos
    7. Fraude
        1. Phishing
4. Medio
    1. Contenido abusivo
        1. Discurso de odio
    2. Obtención de información
        1. Ingeniería social
    3. Intento de intrusión
        1. Explotación de vulnerabilidades conocidas
        2. Intento de acceso con vulneración de credenciales
    4. Intrusión
        1. Compromiso de cuentas sin privilegios
    5. Disponibilidad
        1. Mala configuración
    6. Fraude
        1. Uso no autorizado de recursos
        2. Derechos de autor
        3. Suplantación
    7. Vulnerable
        1. Criptografía débil
        2. Amplificador DDoS
        3. Servicios con acceso potencial no deseado
        4. Reveleación de información
        5. Sistema vulnerable
5. Bajo
    1. Contenido Abusivo
        1. Spam
    2. Obtención de información
        1. Escaneo de redes (scanning)
        2. Análisis de paquetes (sniffing)

A su vez, los niveles de impacto los podemos clasificar en:

1. Crítico:

1. Afecta apreciablemente a la Seguridad Nacional.
2. Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas.
3. Afecta a una Infraestructura Crítica.
4. Afecta a sistemas clasificados SECRETO.
5. Afecta a más del 90 % de los sistemas de la organización.
6. Interrupción en la prestación del servicio superior a 24 horas y superior al 50 % de los usuarios.
7. El ciberincidente precisa para resolverse más de 100 Jornadas-Persona.
8. Impacto económico superior al 0,1 % del P.I.B. actual.
9. Extensión geográfica supranacional.
10. Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.

2. Muy alto:
    1. Afecta a la seguridad ciudadana con potencial peligro para bienes materiales.
    2. Afecta apreciablemente a actividades oficiales o misiones en el extranjero.
    3. Afecta a un servicio esencial.
    4. Afecta a sistemas clasificados RESERVADOS.
    5. Afecta a más del 75 % de los sistemas de la organización.
    6. Interrupción en la prestación del servicio superior a 8 horas y superior al 35 % de los usuarios.
    7. El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona.
    8. Impacto económico entre el 0,07 % y el 0,1 % del P.I.B. actual.
    9. Extensión geográfica superior a 4 CC.AA. o 1 T.I.S.
    10. Daños reputacionales a la imagen del país (marca España).
    11. Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.
3. Alto:
    1. Afecta a más del 50 % de los sistemas de la organización.
    2. Interrupción en la prestación del servicio superior a 1 hora y superior al 10 % de usuarios.
    3. El ciberincidente precisa para resolverse entre 5 y 30 Jornadas–Persona.
    4. Impacto económico entre el 0,03 % y el 0,07 % del P.I.B. actual.
    5. Extensión geográfica superior a 3 CC.AA.
    6. Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
4. Medio
    1. Afecta a más del 20 % de los sistemas de la organización.
    2. Interrupción en la presentación del servicio superior al 5 % de usuarios.
    3. El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona.
    4. Impacto económico entre el 0,001 % y el 0,03 % del P.I.B. actual.
    5. Extensión geográfica superior a 2 CC.AA.
    6. Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
5. Bajo:
    1. Afecta a los sistemas de la organización.
    2. Interrupción de la prestación de un servicio.
    3. El ciberincidente precisa para resolverse menos de 1 Jornadas-Persona.

4. Impacto económico entre el 0,0001 % y el 0,001 % del P.I.B. actual.
5. Extensión geográfica superior a 1 CC.AA.
6. Daños reputacionales puntuales, sin eco mediático

6. Sin impacto.

7.2 Mecanismos de defensa

Los mecanismos de defensa implementan actividades para:

- Detectar y analizar ataques y actividades maliciosas
- Prevenir y mitigar ciberataques
- Recuperar y restaurar los sistemas a la situación anterior al ataque

Estas actividades comprenden:

1. Instalación de herramientas antimalware en todos los equipos informáticos de la organización
2. Contraseñas: uso de políticas seguras (logintud, requisitos, caducidad...)
3. Uso de tecnologías RAID en equipos críticos (servidores, directivos, CTO...)
4. Sistemas de backup en red (NAS) o en la nube
5. Control de acceso y listas de control o ACL a recursos (política del mínimo privilegio)
6. Instalación de firewalls avanzados o NOC (Centro de Operaciones de Red)
    1. Defensa en profundidad y la DMZ
    2. Firewalls
    3. IPS/IDS
    4. EDR (endpoint detection and response) / XDR (detección y respuesta extendidas)
    5. Segregación de redes (usando switches inteligentes, VLAN...)
    6. Protocolos de comunicación seguros
    7. Cifrado de las comunicaciones
7. Implementación del SOC (Centro de Operaciones de Ciberseguridad) y su corazón: el SIEM

Para reforzar la protección, podemos además de lo anterior introducir múltiples capas de seguridad, lo que reduce la probabilidad de compromiso. Estas capas se pueden implementar mediante tres estrategias:

1. En el software de comunicación
2. Establecer dimensiones de profundidad
3. Crear una defensa en profundidad horizontal

7.2.1 Introducción al SOC

En este apartado vamos a hacer una primera aproximación a lo que en un futuro será el SOC (Centro de Operaciones de Seguridad) y cómo podemos crear uno en nuestro homelab.

El personal técnico e ingenieros del SOC llevan a cabo una serie de funciones como son:

- Monitoreo 24/7/365 del entorno completo de la empresa
- Mantenimiento preventivo y despliegue de aplicaciones de seguridad
- Clasificación de alertas para determinar la prioridad durante la respuesta a incidentes
- Respuesta a amenazas
- Contención y erradicación de amenazas
- Análisis de la causa raíz de los incidentes
- Evaluación y gestión del cumplimiento del marco legal (compliance)

Dentro del SOC (Security Operation Center) una pieza clave es el SIEM (Security information and event management). Algunos SIEM incluyen inteligencia artificial para automatizar la tarea de detección, prevención y, en ocasiones, contención bloqueando accesos. Con estas detecciones, los

analistas del SOC harán la contención y erradicación de las amenazas y con los datos recopilados en el SIEM podrán investigar el evento.

Así un SIEM es una colección de componentes usados para monitorear el tráfico de red y los recursos. Desde el punto de vista del usuario, se trata de un tablero (dashboard) con información de seguridad que muestra alertas de actividad sospechosa a un analista de seguridad. Los componentes del SIEM son:

- Agregación de registros de múltiples fuentes
- Inteligencia de amenazas
- Correlación de eventos y su organización para mejor análisis
- Visualización avanzada de datos de analítica
- Algún tipo de tecnología de caza de amenazas (threat hunting) para encontrar recursos comprometidos
- Herramientas forenses para la investigación post-incidente

Como puede imaginar el lector, esta compleja tarea no siempre va a poder estar aglutinada bajo una misma aplicación, sino que trabajaremos con una serie de herramientas que vamos a ir preparando en este tema y desarrollando en los siguientes.

Para implementar el SIEM, el corazón de nuestro SOC, usaremos como máquina base un Ubuntu Server, aunque bien podríamos haber usado Centos, Open SUSE o RHEL. Ubuntu Server es fácilmente virtualizable o también lo podemos usar directamente sobre el hardware ("baremetal"). Sobre ésta instalaremos la pila ELK que veremos con más detalle más adelante. En el momento de redactar este capítulo, comienza a tomar fuerza el proyecto OpenSearch [https://opensearch.org/], un fork de Elasticsearch por el cambio de licencia, en pocos meses podría convertirse en una buena alternativa a ELK.

Como es una pieza fundamental y muy delicada del corazón de nuestra estructura de ciberseguridad, siempre que sea posible haremos la instalación desde una ISO oficial a la que previamente verifiquemos el hash.

Para reducir el tiempo de instalación también podemos usar una máquina ya creada de Linux VM Images. Disponen de imágenes para VirtualBox y VMWare aunque de la versión "Desktop". En el caso que el homelab de casa lo tengamos con ProxMox, podemos descomprimir el archivo (recuerdo que los OVA son ficheros tar que se pueden extraer con el flag "x": tar x fichero.ova) y luego importar el disco.

Para usar una máquina virtual de Internet en Proxmox, podemos descargarla con *wget* o un gestor como *axel*, descomprimir el archivo con *bsdtar x -f fichero*, creamos una máquina virtual sin disco y luego se lo importamos con *qm importdisk VM-ID fichero.vmdk local-lvm -format qcow2*.

Otra interesante opción para gestionar máquinas virtuales si no disponemos de una máquina dedicada para ello, es Vagrant.

Una vez descargada y funcionando actualizamos la máquina antes de seguir:

```
apt update
apt upgrade
```

Asegúrate que la hora está sincronizada con el huso horario en el que estamos, para ello puedes ver la hora local con **date** desde la terminal y, si fuera necesario, puedes corregir la hora con **# dpkg-reconfigure tzdata**.

La pila ELK

La pila ELK (ELK Stack) es la combinación de tres herramientas software libre en una: Elasticsearch, Logsatsh y Kibana. Logstash se encarga de la ingesta de datos de registros (logs) de

servicios y sistemas y también de paquetes capturados de red en la base de datos Elasticsearch para luego ser visualizados y analizados mediate la interfaz de Kibana.

Es importante entender que Elasticsearch no es una aplicación de escritorio, ni tan siquiera para trabajar sólo en un equipo, es un sistema pensado fundamentalmente para complejas consultas sobre ingentes cantidades de datos (tiene que ver, como podríamos sospechar, también con el "*big data*") . Elasticsearch es un motor de búsqueda escrito en Java que funciona sobre Apache Lucene, una API para un motor de búsqueda de alto rendimiento. Elasticsearch nos permite acceder a Lucene como una API REST distribuida y escalable, en vez de con complicadas llamadas en Java, así los verbos HTTP GET, POST, PUT, DELETE, por ejemplo, nos servirán para consultar, crear, actualizar y borrar documentos JSON en nuestra base de datos NoSQL.

Como hemos dicho antes, Elasticsearch no es una aplicación para ejecutar como un único demonio (aunque puede hacerse) si no distribuida. Así, cada instancia de Elastic que corre en un servidor será un **nodo**. Existen diferentes tipos de nodos:

- El nodo encargado de orquestrar al resto será el **nodo maestro** y lleva la pista de cómo se van particionando los datos entre nodos y fragmentos (**shards**).
- Los nodos de datos o **data nodes** son los encargados de llevar a cabo las operaciones CRUD (Create Read Update Delete) y también actúan en las búsquedas y agregaciones de datos.
- Los nodos encargados de la ingesta de datos son los **nodos de ingesta**. Llamamos *ingesta* al proceso de enriquecer y transformar información antes de indexarla. Aunque los datos pueden provenir de una tubería (*pipeline*) o bien de ficheros estáticos, el sentido de estos nodos es gestionar la información que llega desde las diferentes fuentes o *pipelines* (tuberías) en vivo.
- Los nodos *ML* o **machine learning** son los encargados de ejecutar tareas de aprendizaje automático, aunque para esta característica deberemos adquirir una licencia previo pago.

De este modo un **clúster** de Elasticsearch consiste en un conjunto de uno o más nodos que trabajan conjuntamente. Las ventajas de usar un clúster frente a un único nodo son múltiples: tolerancia a fallos, mayor velocidad, capacidad para almacenar y gestionar una mucho mayor cantidad de información...

Sea cual sea la configuración de nuestro servicio Elasticsearch, la información será almacenada como documentos consistentes en un **documento JSON** con el formato clave-valor, donde la clave es el nombre del campo y el valor es el dato almacenado para ese campo en particular. Como en cualquier base de datos NoSQL, no hay limitaciones para el formato de estos documentos, a diferencia de un sistema de base de datos relacional donde previamente hemos de fijar los campos y el tipo de información que van a almacenar.

Para simplificar la tarea de la recuperación de documentos, Elasticsearch permite un espacio de nombre lógico común para todos los documentos del mismo tipo, por ejemplo, supongamos que queremos almacenar la información del fichero access.log de un servidor Apache, estos registros pueden almacenarse en un mismo **índice** (por ejemplo que llamemos *"apache"*) para facilitar posteriormente su consulta.

La arquitectura distribuida de Elasticsearch es posible gracias a los fragmentos o **shards**, que simplemente son un *índice totalmente funcional de Lucene*. Así por ejemplo, tenemos 50 GB de datos del pipeline del fichero *eve.json* de nuestro *IDS Suricata*. Podemos partirlos en 5 fragmentos de 10 GB lo que permite hacer complejas consultas o procesado en tiempo real.

Instalación de ELK Ubuntu Server

Para instalar la pila ELK en nuestro servidor Ubuntu podemos usar el repositorio oficial que nos ayudará a mantener nuestro software acualizado sin necesidad de complicados scripts:

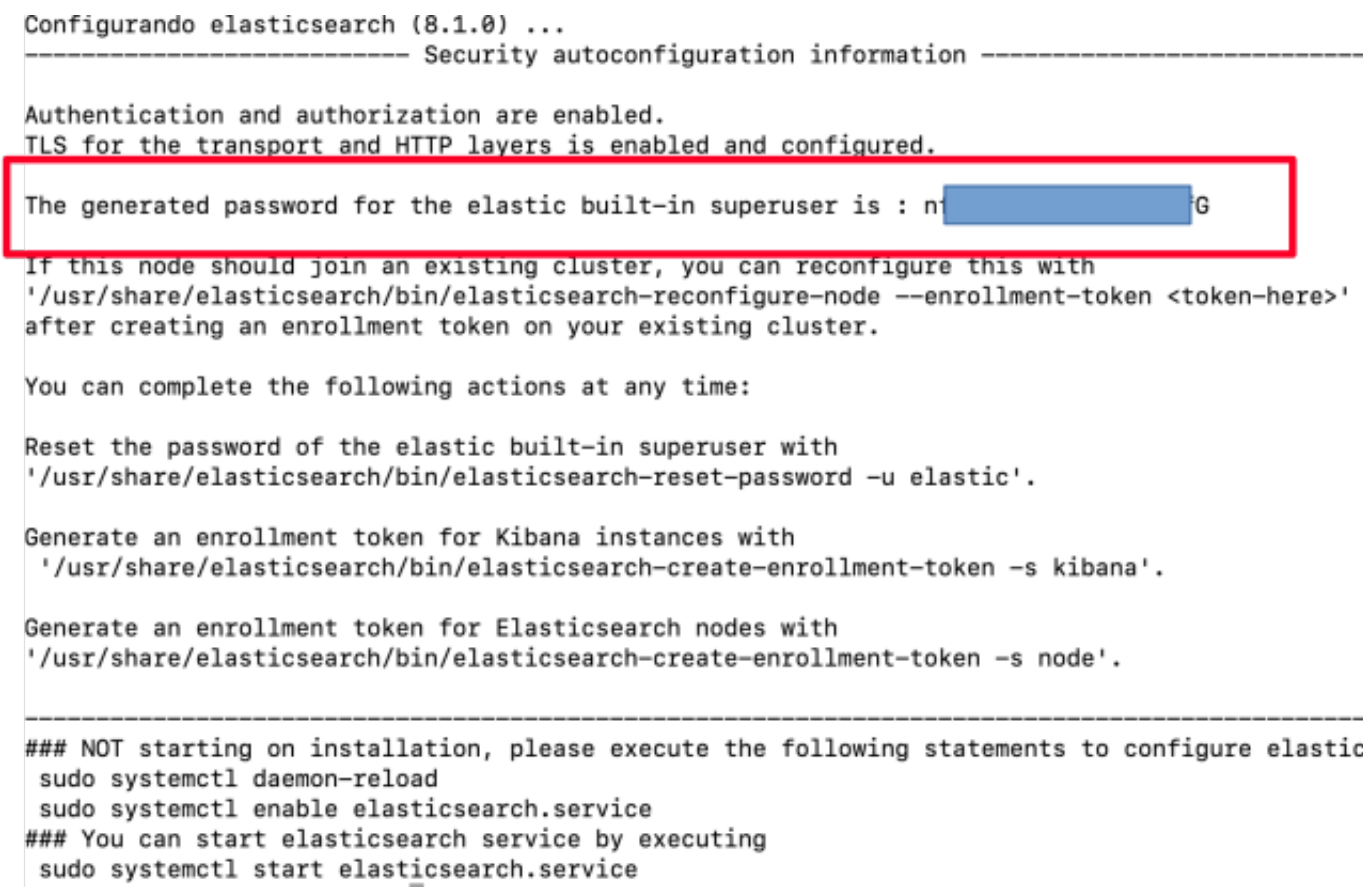


Figura 7.1: En esta versión durante la instalación muestra el password generado

```
# FUENTE: https://www.elastic.co/guide/en/elasticsearch/reference/current/deb.

wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key a
sudo apt-get install apt-transport-https
echo "deb␣https://artifacts.elastic.co/packages/8.x/apt␣stable␣main" | sudo te

echo "IMPORTANTE:␣APUNTA␣EL␣PASSWORD␣QUE␣ES␣COMUNICADO␣A␣CONTINUACION"

sudo apt-get update
sudo apt-get install elasticsearch
sudo apt-get install kibana
sudo apt-get install logstash

sudo /bin/systemctl daemon-reload
sudo /bin/systemctl enable elasticsearch.service
sudo /bin/systemctl enable kibana.service

sudo systemctl start elasticsearch.service
```

En esta versión durante la instalación muestra el password generado, luego hay que tener la precaución de anotarlo para no tener que resetearlo desde la línea de comandos:

Antes de lanzar kibana, hemos de saber que para poder conectarnos o bien hacemos un tunel SSH, por ejemplo con **ssh -L 5601:localhost:5601 usuario@ubuntu**, o bien configuramos para que cualquier host de nuestra red pueda verlo cambiando el *server.host* a la IP de la máquina virtual en el fichero de configuración */etc/kibana/kibana.yml*.

```
sudo systemctl start kibana.service
```

Si disponemos de una máquina con recursos limitados (por ejemplo una Raspberry Pi -al menos de 4 GB de RAM- o una máquina virtual en un hardware con poca RAM y procesador) podemos reducir el consumo de RAM de ELK modificando las opciones de la máquina virtual Java (ojo, para ello hay que usar Java). En Elastic 8.x creamos el fichero **/etc/elasticsearch/jvm.options.d/mem.options** y le añadirmos estas líneas para limitar el tamaño del heap a 2GB:

´´´bash -Xms2g -Xmx2g ´´´

Elastic no debería ocupar más de la mitad de la memoria del hosts para evitar problemas de rendimiento, aunque para producción son recomendados unos 30 GB de RAM disponibles sólo para el servicio (es decir se recomienda una máquina con 64 GB de RAM).

Igualmente podemos hacer con logstash en fichero **/etc/logstash/jvm.options** y kibana, aunque en este último al ser un programa para node.js es un poco distinto, sería en el fichero **/etc/kibana/-node.options** y habría que descomentar la línea donde pone *–max-old-space-size=4096*.

7.2.2 IDS Snort

Snort es un sistema de detección de intrusiones (IDS) y sistema de prevención de intrusiones (IPS) creado en 1998 y ahora mantenido por CISCO.

7.2.3 Bastionado de redes: Network Security Monitoring (NSM)

7.2.4 Security Onion

Security Onion es una completa suite de auditorías de redes completamente gratuita y de código abierto. Se trata de una distribución Linux orientada a la detección de amenazas, monitorización de seguridad y gestión de los logs. Cuenta con múltiples herramientas incluidas por defecto, por lo que no tendremos que es muy rápida su puesta en marcha. Por ejemplo, tenemos ya configuradas y funcionando herramientas como Elasticsearch, Snort, Zeek, Wazuh, Cyberchef y NetworkMiner entre otras herramientas. Por otro lado, es muy sencilla de implementar, porque cuenta con un asistente de instalación que permite que en minutos esta suite se ponga en marcha.

Una de las razones por las cuales Security Onion debe ser considerada para las auditorías de redes y seguridad, es la capacidad de juntar múltiples herramientas con gran reputación en seguridad en redes en un sólo paquete. Esto no solamente lo hace más sencillo de administrar, sino que también facilita el acceso a organizaciones de todo tipo a una solución integral. Es decir, una solución completa que garantice que los responsables de la infraestructura y seguridad de las redes tengan el panorama completo.

Además no sólo contiene herramientas reactivas, como, por ejemplo, las de respuesta a incidentes o seguridad informática forense. También contiene herramientas proactivas que nos ayudan a saber qué pasa con nuestra red. Qué vulnerabilidades tiene con diferentes escáneres de vulnerabilidades, qué puertos están abiertos sin necesidad y un largo etcétera.

Para probar SecurityOnion y evitar el tiempo de *fontanería*, podemos usar su CD de instalación que está disponible en (`https://github.com/Security-Onion-Solutions/securityonion/blob/master/VERIFY_ISO.md`), creando una máquina virtual.

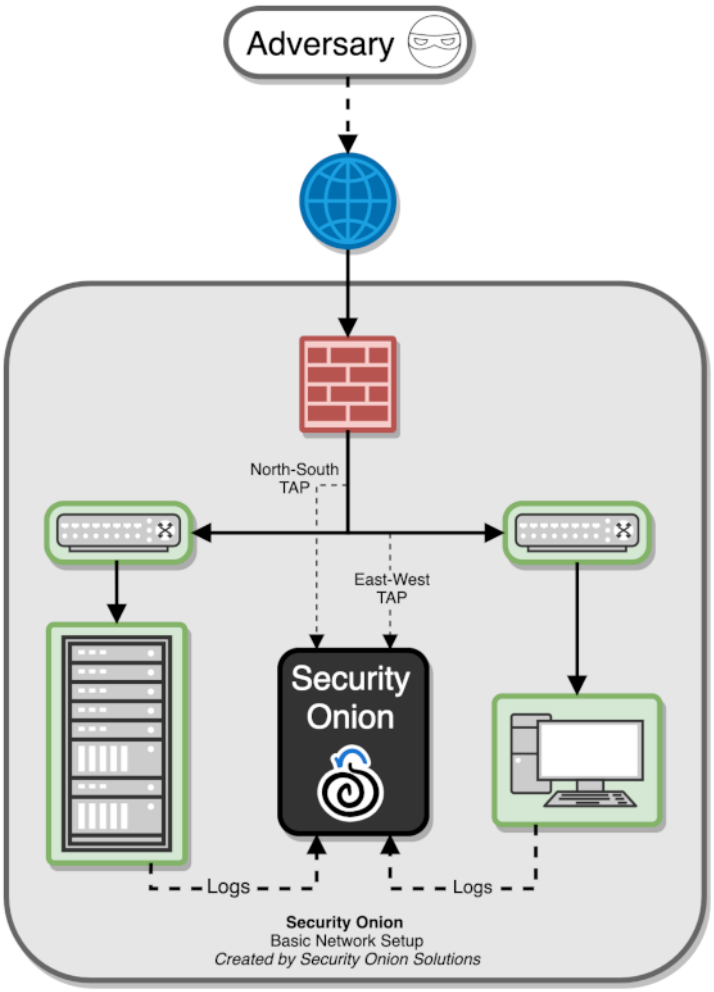


Figura 7.2: Esquema de NSM

7.2.5 Zeek (Bro)

7.2.6 IDS Avanzado

Snort+Sguil+Squert

7.2.7 NOC con pfSense

7.2.8 Servicios de VPN

OpenVPN Server
OpenVPN Client

7.2.9 Snort como IPS en pfSense

La ventaja de correr *snort* dentro del router es que puede bloquear aquel tráfico detectado como malicioso, pasando de ser simplemente un IDS (sistema de detección de intrusiones) a un IPS (sistema de protección contra intrusiones). No obstante, programas como *snort* y *suricata* son propensos a dar falsos positivos o simplemente detectar tráfico *sospechoso* sin más, bloqueando en muchas ocasiones conexiones lícitas.

Debido al alto volumen de peticiones o al uso de verbos HTTP de manera un tanto extraña, es muy común tener problemas con asistentes virtuales (dispositivos Alexa, Homepod, Google Home...), dispositivos IoT o Webs de recursos en la nube como Google Suite, Google Classroom, también a la hora de actualizar sistemas operativos...

Para llegar a un buen equilibrio entre seguridad y funcionalidad es necesario hilar muy fino y añadir listas de IPs

7.2.10 NETFLOW

7.3 Mitre ATT&CK

Mitre ATT&CK (ATT&CK - Adversary Tactics, Techniques and Common Knowledge) propone matrices de conocimiento común de tácticas y técnicas del adversario; que no es más que un modelo de comportamiento del ciber-adversario donde se reflejan las distintas fases del ciclo vital de un ataque genérico. El modelo proporciona una taxonomía común de acciones adversas individuales entendidas por los lados ofensivo y defensivo de la ciberseguridad. También proporciona un nivel apropiado de categorización para la acción del adversario y formas específicas de defenderse contra ella. Se trata de una manera de enfocar los ciberataques. En lugar de mirar los resultados de un ataque, también conocido como un indicador de compromiso (IoC), los analistas de seguridad deben considerar las tácticas y técnicas que indican que un ataque está en progreso. Las tácticas son el por qué de una técnica de ataque. Las técnicas representan cómo un adversario logra un objetivo táctico al realizar una acción. El conocimiento común es el uso documentado de tácticas y técnicas por parte de los adversarios. Esencialmente, es la documentación de *tácticas, técnicas y procedimientos* o TTP.

MITRE tiene ATT&CK disponible en dos matrices diferentes:

- Enterprise: [`https://attack.mitre.org/matrices/enterprise/`]. Se compone de técnicas y tácticas que se aplican a los sistemas Windows, Linux o MacOS.
- Mobile: [`https://attack.mitre.org/matrices/mobile/`]. Esta matriz contiene tácticas y técnicas que se aplican a los dispositivos móviles.

Anteriormente también existía una matriz PRE-ATT&CK, con las tácticas y técnicas relacionadas con lo que los atacantes hacen antes de intentar vulnerar una red o un sistema en particular, pero ahora está integrada en **Enterprise**.

- **Reconocimiento**: recopilación de información para planificar futuras operaciones del adversario, es decir, crear una base de datos de información sobre la organización objetivo.
- **Desarrollo de recursos**: establecer recursos para respaldar las operaciones, es decir, establecer una infraestructura de comando y control.
- **Acceso inicial**: intentar entrar en la red de la compañía, por ejemplo, mediante spear phishing.
- **Ejecución/infección**: intentar ejecutar código malicioso, es decir, ejecutar una herramienta de acceso remoto.
- **Persistencia**: tratar de mantener su punto de apoyo, es decir, cambiar configuraciones.
- **Escalada de privilegios**: intentar obtener permisos de nivel superior, es decir, aprovechar una vulnerabilidad para elevar el acceso.
- **Evasión defensiva**: tratar de evitar ser detectado, es decir, utilizar procesos confiables para ocultar malware.
- **Acceso a credenciales**: robo de nombres y contraseñas de cuentas, normalmente mediante keyloggers, stealers...
- **Descubrimiento**: tratar de descubrir su entorno, es decir, explorar lo que pueden controlar.
- **Movimiento lateral**: moverse a través de su entorno, es decir, usar credenciales legítimas para moverse por múltiples sistemas.
- **Recopilación**: recopilar datos de interés como almacenamiento en la nube, bases de datos de clientes, etc.
- **Comando y control**: comunicarse con sistemas comprometidos para controlarlos, es decir, imitar el tráfico web normal para comunicarse con una red de víctimas.
- **Exfiltración**: robar datos, es decir, transferir datos a una cuenta en la nube...
- **Impacto**: manipular, interrumpir o destruir sistemas y datos, es decir, cifrar datos con ransomware.

8. Detección de incidentes

8.1 IDS
8.2 SOC
8.3 SIEM

9. Respuesta ante incidentes

9.1 Contención

9.2 Erradicación

9.3 Recuperación

https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/respuesta-incidentes.pdf
https://www.incibe-cert.es/guias-y-estudios/guias/guia-nacional-notificacion-y-gestion-ciberincidentes

10. Actividad postincidente

"Puede que las guerras no se ganen. Puede que simplemente continúen en el tiempo.". Mr Robot.

10.1 Documentación, evidencias y ciclo de mejora

V

Quinta Parte

11 Inteligencia artificial 101
11.1 Inteligencia artificial aplicada a la ciberresiliscencia

11. Inteligencia artificial

11.1 Inteligencia artificial aplicada a la ciberresiliscencia

VI Bibliografía, webs y programas recomendados

Bibliography 105
Articles
Books
Books
Books

Bibliografía y enlaces de interés

Bibliografía
Webgrafía
Grupos de Telegram
Software para DFIR