

BLOQUE DE

CIBERSEGURIDAD

INDICE

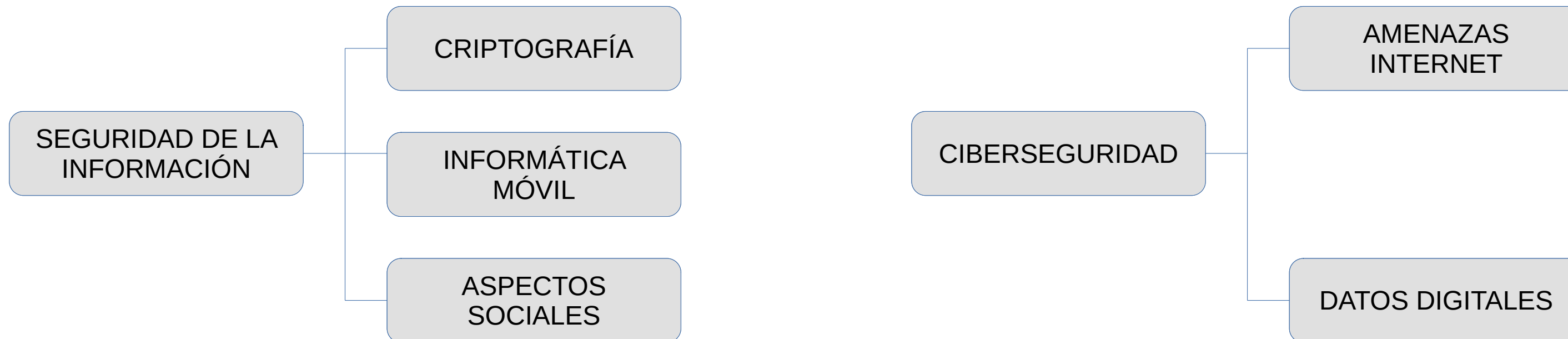
1. Conceptos básicos de ciberseguridad
2. Principales amenazas en Internet
3. Herramientas y soluciones de ciberseguridad
4. Marcos de gestión para la prevención, protección, respuesta y gobierno

Comencemos...



¿Qué es la ciberseguridad?

- Prevenir y detectar uso no autorizado de un sistema informático
- Seguridad informática → rama de la seguridad de la información



Objetivos de la seguridad informática

1. Confidencialidad
2. Integridad
3. Disponibilidad
4. Autenticación
5. No repudio



¿¿Por qué es importante la seguridad informática??



Algunos casos famosos sólo en 2023:

- Brecha de seguridad de 37 millones de clientes de T-Mobile
- Fuga de datos de Activision
- Mailchimp confirma haber sufrido un ataque de ingeniería social que puso en riesgo las cuentas de 133 clientes
- Unos hackers han atacado la fábrica de Suzuki. Llevan 10 días parados y han perdido más de 20.000 motos
- Un ciberataque a un proveedor está detrás de la brecha de datos de Discord
- Reddit confirma haber sufrido un ataque de 'phishing', pero insiste en que los datos de los usuarios están seguros
- Ataque Cibernético a Toyota: Hackers habrían filtrado 3,1 millones de datos sensibles de clientes.

¿Qué protege la seguridad informática?

- 1) Información
- 2) Equipamiento físico
- 3) Redes y comunicaciones/infraestructura
- 4) Usuarios



Tipos de seguridad

1. Seguridad lógica: Protege software e información

2. Seguridad física: Protege el hardware ante desastres naturales

o accidentes

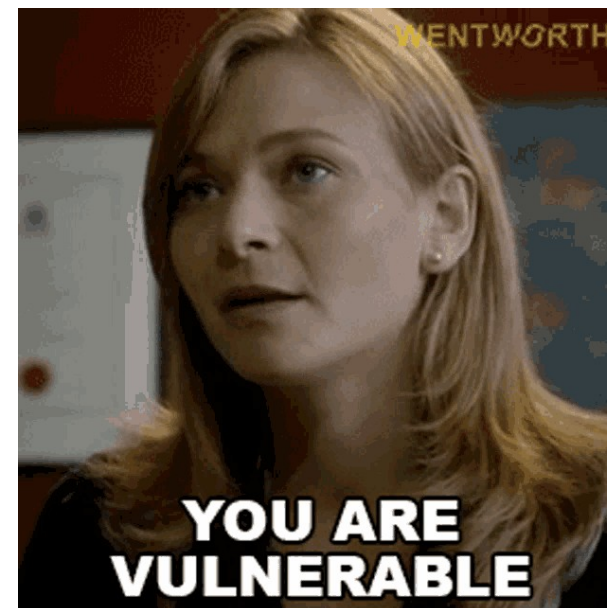
Incendio en la sede de
OVH de Estrasburgo, uno
de los proveedores de
hosting más importantes de
Europa

Tipos de seguridad

1. Seguridad activa: Previene daños de cualquier tipo, tanto físicos como lógicos
2. Seguridad pasiva: Intenta paliar el daño cuando las medidas de seguridad activa no han sido efectivas

Amenazas y vulnerabilidades

1. Vulnerabilidad: debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información → [Ejemplos en 2023](#)



Amenazas y vulnerabilidades

2. Amenaza: acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información

- Fraude, robo, virus
- Sucesos físicos
- Negligencia o decisiones institucionales

Amenazas y vulnerabilidades

El riesgo depende de:

- Probabilidad de que se consume una amenaza
- Esta amenaza a su vez depende de una vulnerabilidad
- Se produce un daño



Fuentes de amenazas más comunes

- Malware o código malicioso
- Ingeniería social
- APT o Amenazas Persistentes Avanzadas
- Botnet
- Redes sociales
- Servicios en la nube

Riesgos

- Se deben identificar los activos más críticos de un sistema de información → Análisis de riesgos → Sus fases son



Riesgos

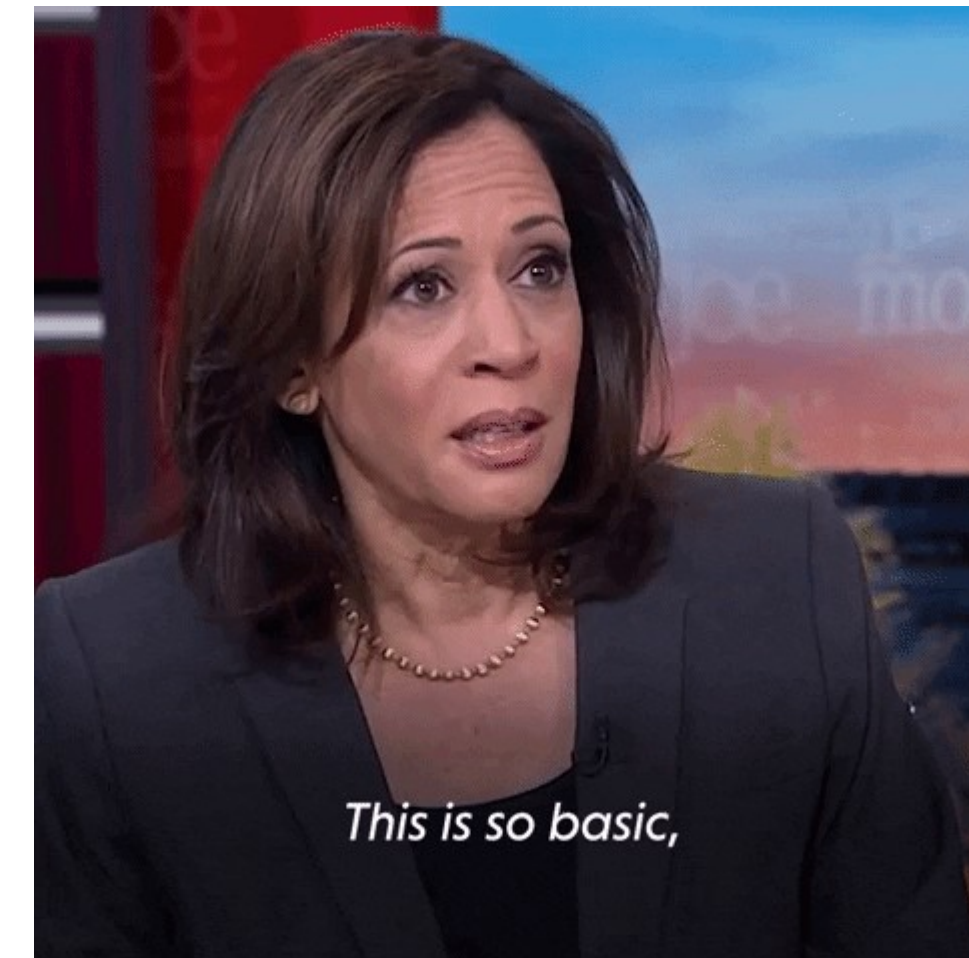
- El análisis de riesgos nos permite estimar la magnitud y la gravedad del riesgo al que está expuesta la organización
- Estableceremos un umbral de riesgos que nos ofrecerá varias opciones:
 - Evitar el riesgo
 - Adoptar soluciones para minimizar el impacto o la probabilidad del riesgo
 - Compartir/transferir el riesgo
 - Aceptar el riesgo

Política de seguridad

- Tras identificar activos y evaluar riesgos → política para protegerlos
- Política → Documento de alto nivel **aprobado por la directiva**
- Ejemplo de puntos que pueden quedar recogidos:
 - Controles acceso físico
 - Controles acceso lógico
 - Clasificación información por importancia
 - Gestión incidentes seguridad

Protección de la información

- **Consejos básicos:**
 - Control de accesos
 - Cifrado de la información
 - Eliminación de la información
 - Limitar uso herramientas no autorizadas
 - Cláusulas legales
 - Backups
 - Contraseñas fuertes
 - Herramientas adecuadas protección
 - Sentido común





Principales amenazas en Internet

Comencemos...



Introducción

- Las ciberamenazas son importantes para todas las empresas pero... en las PYMES es más notorio por la falta de recursos.
- Especialmente importante en las PYMES industriales
- Gran coste económico  
- Proteger la información a toda costa

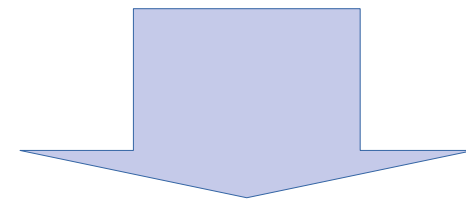
Ransomware

- Tipo de malware más lucrativo últimos años
- Principal ciberamenaza
- Infecta red empresarial y cifra todos los archivos
- Demanda un rescate para descifrarlos
- ¿Un rescate de 70 millones de \$\$\$?!



Ransomware

- Ha sufrido una evolución en el tiempo → Se ha sofisticado



- Se crean campañas de ramswomware ad-hoc
- Cifrar todos los archivos consume tiempo y recursos → Se pasa a la extorsión

Ataques a la disponibilidad de servicios (DoS/DDoS)

Objetivo: Colapsar el servicio ofrecido por un servidor o red → Inundándolo de tráfico o peticiones hasta sobrepasar capacidad

DDoS

- La D hace referencia a *Distributed* o distribuido.
- El tráfico proviene de muchos orígenes distintos → Normalmente *botnets* → Formadas por ordenadores *zombies*

Desinformación: fake news, astroturfing

- El astroturfing tiene como fin manipular opiniones para alterar el mercado y la libre competencia
- Se sirve de una parte emocional y también de una racional
- Normalmente utilizada con fines políticos → También puede suponer un riesgo para las empresas



ASTROTURFING CONTRA TIKTOK PAGADO POR META (FACEBOOK)



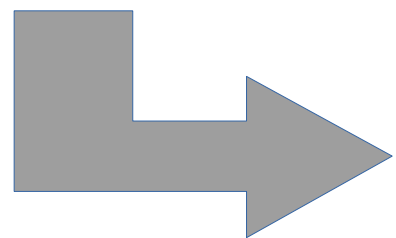
Tenía pendiente dedicar una pieza a la que fue la bomba informativa de la semana pasada: Meta, la empresa matriz de Facebook, WhatsApp, Instagram y compañía, pagó a Targeted Victory, una firma de consultoría republicana, para que esta se encargase de desprestigiar mediáticamente a TikTok (EN).

Ataques contra la cadena de suministro

- También conocidos como ataques a la cadena de valor o ataque a terceros
- Ataques cada vez más populares
- No se producen contra la empresa objetivo, sino contra uno de sus proveedores
- Aumenta superficie de ataque



¿Cómo funcionan?



- Los atacantes escanean al objetivo en busca de un punto de entrada e introducen malware en el proceso de producción del producto.
- El software “con sorpresa” queda legitimado por el proveedor de forma aparentemente normal

Ataques contra la cadena de suministro

Ejemplos

- **SolarWinds:** empresa que comercializa software Orion para monitorizar y administrar infraestructura IT
- En 2020 un actor malicioso introdujo un *backdoor*
- Se tuvo acceso a datos de 33000 clientes
- **Equifax:** 2 billones (USA) de daño.
- **ASUS:** Infectado un software preinstalado en sus ordenadores

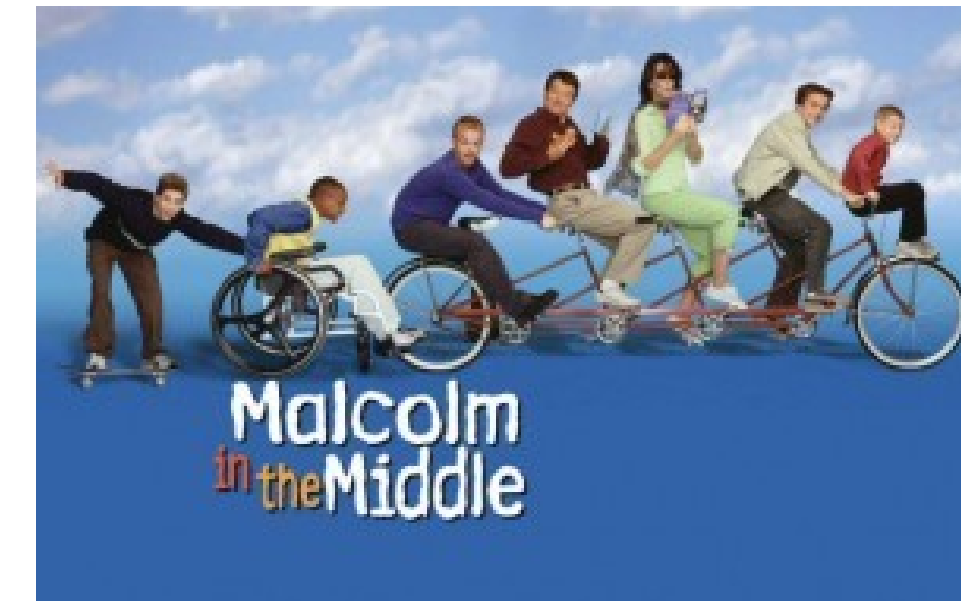
Ataques contra la cadena de suministro

Defensas

- Mínimo privilegio
- Segmentación de red
- Integrar seguridad dentro del ciclo de desarrollo
- Monitorización

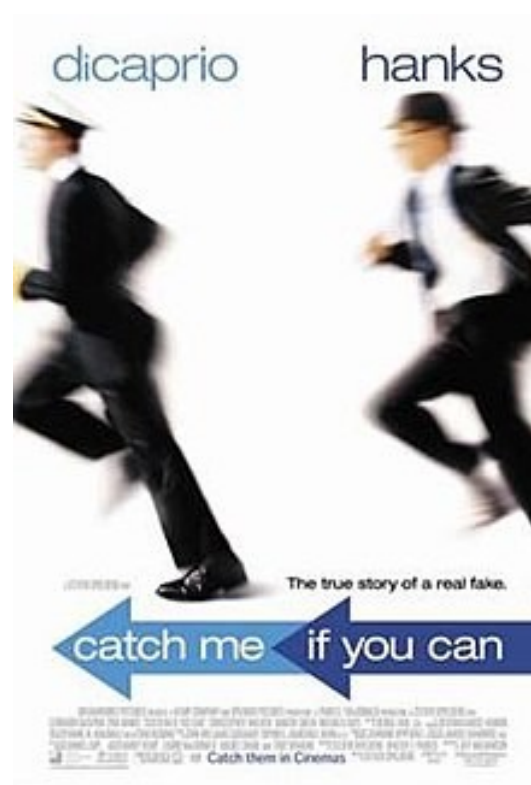
Man in the Middle (MITM)

- El cibercriminal se interpone en una transacción entre dos partes
- Puede filtrar o robar datos
- Se pueden paliar estos ataques:
 - Cifrando comunicaciones
 - Autenticación multifactor



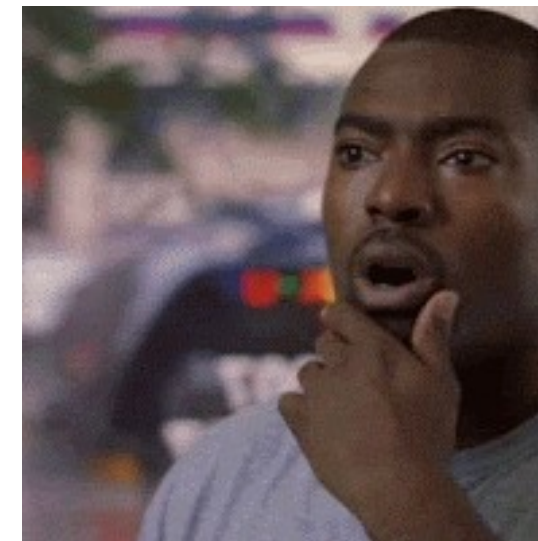
Ingeniería social

- Es la versión moderna de los estafadores o timadores
- Atacantes utilizan sugestión para ganar confianza de usuarios autorizados
- Se aprovechan de la naturaleza bondadosa y de la predisposición de la gente a ofrecer ayuda



Phising

- Hace uso de la ingeniería social
- Emails o SMS
- Dentro del mensaje suele haber un link falso para introducir información



Spear phishing

- Ataques de phishing pero dirigidos para aumentar probabilidades
- Se lleva a cabo una investigación del objetivo o víctima
- El mensaje aparecerá como más convincente y aumenta tasa éxito

Ejemplo

El atacante simulando ser del dpto. de informática pidiendo hacer click en algún sitio

Smishing y vishing

- **Vishing**: Fraude de carácter telefónico



- **Smishing**: Fraude haciendo uso de mensajes SMS



Whaling

- Tipo de *phishing* muy específico → *spear phishing* muy focalizado
- El objetivo en este caso es un ejecutivo de muy alto nivel
- Se realiza una investigación previa y tras ello se envía el email
- Los emails se apoyan en la confianza usando información personalizada
- En ocasiones incluso se acompaña de una llamada telefónica para apoyar el relato
- Consecuencias catastróficas → Gran pérdida económica hasta exfiltración de datos

Protegerse del phishing

- Desconfiar ante emails “raros”
- Intentar se racional
- Comprobar remitente o URLs adjuntas
- Evitar descargar imágenes o archivos si se tiene duda

SQLi – SQL injection (Inyección SQL)

- Si tenemos información almacenada en una base de datos necesitaremos consultarla o modificarla
- Para acceder a la BBDD y a la información que hay dentro, utilizamos un lenguaje descriptivo → SQL (Structured Query Language)
- Se introducen partes maliciosas en las consultas SQL para obtener acceso a toda la base de datos
- Es un ataque muy popular desde hace muchos años → ¿La protección está muy avanzada...?
- Todavía sigue siendo muy popular



FMANUEL @fdotmanuel

3 Junio 2011 — Actualizado 4 Junio 2011, 12:06

El ciberataque contra los Mossos d'Esquadra se valió de una vulnerabilidad Web

El hacker que reivindicó la acción del pasado 19 de mayo, aprovechó la vulnerabilidad de la Web para difundir los datos personales de 5.540 agentes, introduciendo código a través de formularios, lo que se conoce como SQL Injection.

Los problemas de seguridad de Sony persisten. Tras el [robo de datos bancarios perpetrado contra Sony Online Entertainment](#), ahora le ha tocado el turno a Sony Pictures Entertainment. El grupo de hackers conocido como LulzSec se atribuye el **robo de datos personales de un millón de usuarios de Sony Pictures Entertainment**, la división de cine de Sony.

La fuente indica que la técnica empleada para el ataque ha sido la conocida como *SQL injection*. De esta forma han comprometido la información personal de más de 1.000.000 de usuarios, incluyendo contraseñas, direcciones de correo electrónico, direcciones postales y fechas de nacimiento.

Ataques de contraseñas

- Vector de ataque típico
- Una de las formas más comunes de la que se comprometen los sistemas
- Un password comprometido puede tener grandes repercusiones como fraude financiero, un DDoS o el robo de información sensible.



Tipos de ataques de contraseñas

- Phishing
- Fuerza bruta:
 - Probar distintas combinaciones hasta dar con la correcta
 - Método antiguo y a lo *bruto* pero con las tarjetas gráficas actuales la potencia de cómputo se ha multiplicado
 - Fácil de automatizar

Formas de combatirlo:

- Limitar intentos de acceso en un lapso de tiempo
- Limitar intentos provenientes de la misma IP en un lapso de tiempo
- Contraseñas fuertes

Ataques de diccionario

- Se utiliza una lista o diccionario que son susceptibles de ser usados como password.
- Esta lista se elabora analizando los patrones y comportamientos a la hora de establecer contraseñas en otros ataques que hayan tenido éxito
- Existen listas legales de passwords comunes

Prevención

- No usar “palabras de diccionario” como contraseña
- Bloquear cuentas después de varios intentos fallidos
- Utilizar gestor de contraseñas



Password spraying

- Técnica que hace referencia a, cuando se produce una brecha de seguridad, intentar reutilizar las credenciales comprometidas en otros servicios o lugares



Keylogging

- Software/Hardware
- Permite a un atacante registrar las pulsaciones de teclas en un ordenador
- Toda pulsación queda registrada

Prevención

- Examinar físicamente el ordenador
- Usar antivirus/EDR
- Autenticación multifactor

Internet de las cosas – IoT (Internet of Things)

- Con la llegada del 5G → eclosión del IoT
- El IoT hace referencia a que cualquier dispositivo común de nuestra vida diaria esté conectado a Internet (bombillas, smart watches, dispositivos médicos...)
- Tecnología poco madura → Aún no hay mucho énfasis en su seguridad



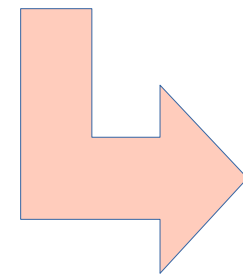
Puede llegar a ser muy peligroso:

- [Mirai](#)
- [Cámaras bebés](#)



Emotet

- Malware identificado por primera vez en **2014**
- En su origen → troyano bancario
- Mantuvo un perfil bajo → *Unos cardan la lana y otros se llevan la fama* (Wannacry/Lockbit)



Los platos con más
sustancia se hacen a fuego
lento

No ha parado de evolucionar y sofisticarse



Emotet

- Su principal medio de transmisión fue el email
- Correos que solían incluir archivos de Office infectados o links maliciosos
- Actualmente se ha sofisticado hasta llegar a una arquitectura modular → capaz de contactar con un servidor externo para descargar los módulos que le aporten la funcionalidad deseada:
 - Robo credenciales email
 - Obtener nombres de usuario y contraseñas almacenadas en navegador web
 - DDoS
 - Instalar otros malwares

Emotet

- Nivel de sofisticación **MUY ALTO**
- Automatiza el descubrimiento de la mejor manera para monetizar la infección realizada en función del escenario:
 - ¿Historial navegación?
 - ¿Dispositivo infectado *tope gama*?
 - ¿El dispositivo está en una red con gran ancho de banda?

Herramientas y soluciones de ciberseguridad

Comencemos...



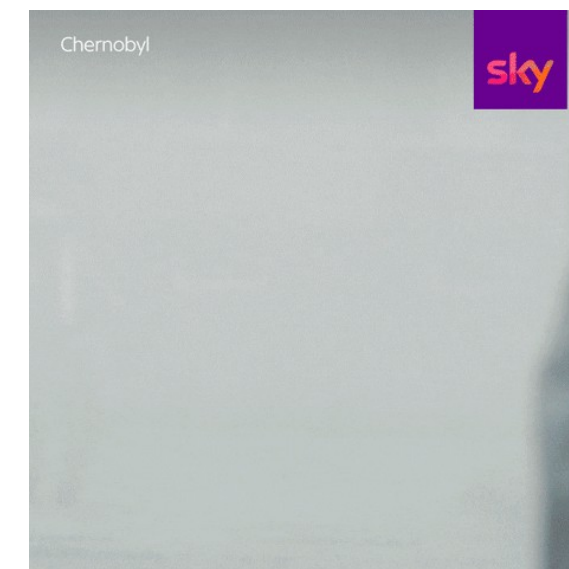
Introducción

- **Recordemos:** el activo más importante de una empresa es la información
- Cibercrimen es muy lucrativo
- Ha habido una gran evolución de legislación y normativa
- Las empresas deben conocer las herramientas y soluciones necesarias
- Se debe reducir la superficie de ataque al mínimo dentro de nuestras posibilidades

Antivirus/EDR/XDR

Antivirus: Software diseñado para detectar y eliminar malware

- Suele ejecutarse en segundo plano → protección en tiempo real
 - Tienen información actualizada de virus conocidos (en ese momento) pero... → ¡OMG! ¡No paran de aparecer amenazas!
 - **Actualizaciones periódicas**
 - Su base de datos contiene ***firmas*** → secuencia de bytes que identifican un virus/malware
 - Si se detecta alguna firma escaneando archivos o carpetas, se identifica como malware → cuarentena o elimina+
-
- Esto que hemos contado hace uso de un **enfoque reactivo** para luchar contra el malware



Antivirus

Los antivirus, con su enfoque reactivo, resultan desfasados en ciertos puntos:

- 1) Firmas de virus ya conocidos → No detectamos virus recientes
- 2) Ventana temporal peligrosa entre descubrimiento de un nuevo virus y la generación de la firma correspondiente
- 3) Nuevos virus emplean técnicas de ofuscación

El otro enfoque que se puede utilizar → Proactivo o **heurístico**

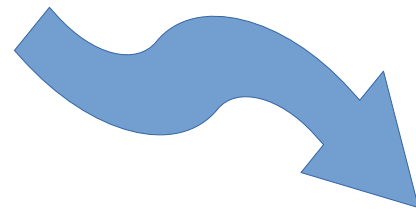
- Método basado en buscar coportamiento sospechosos
- Además este método se divide en dos tipos más:
 1. Estático: Se examina el código del programa
 2. Dinámico: Se utiliza un sistema operativo virtualizado (*sandbox*) aislado para analizar el presunto malware

Antivirus

El método heurístico no sustituye al basado en firmas → Se complementan

Método basado en IA y aprendizaje automático

¡Desventajas!

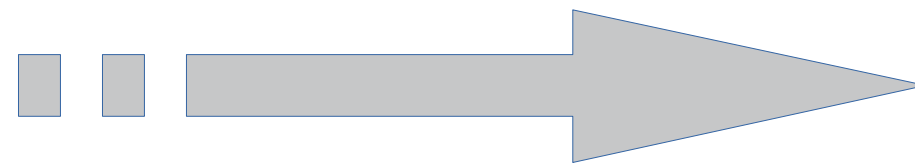


- Falsos positivos
- Recursos necesarios

EDR (Endpoint Detection and Response)

- Herramientas para detectar e investigar amenazas en los endpoints
- Protección por capas
- Monitorización + análisis de datos + Reglas = Respuesta automática

Se denomina endpoint a cualquier dispositivo informático conectado a una red y que se comunica con ella.



Los estudios estiman que un 90% de los ciberataques *exitosos* y un 79% de las fugas de datos se originan en los endpoints.

EDR (Endpoint Detection and Response)

- Pero, pero... ¿¿Cuál es la diferencia con un antivirus??
- Ahora te la cuento:
 1. Recolección continua de datos del endpoint → necesita un *agente*
 2. Análisis y detección en tiempo real → machine learning
 3. Respuesta automática frente a amenazas
 4. Investigación y remediación
 5. *Threat hunting*

Los EDR por lo general buscan dos indicios; los **indicadores de compromiso (IOC)**, que son acciones o eventos que denotan un potencial ataque y los **indicadores de ataque (IOA)** que son eventos que se relacionan directamente con ciberamenazas o ciberdelitos conocidos.

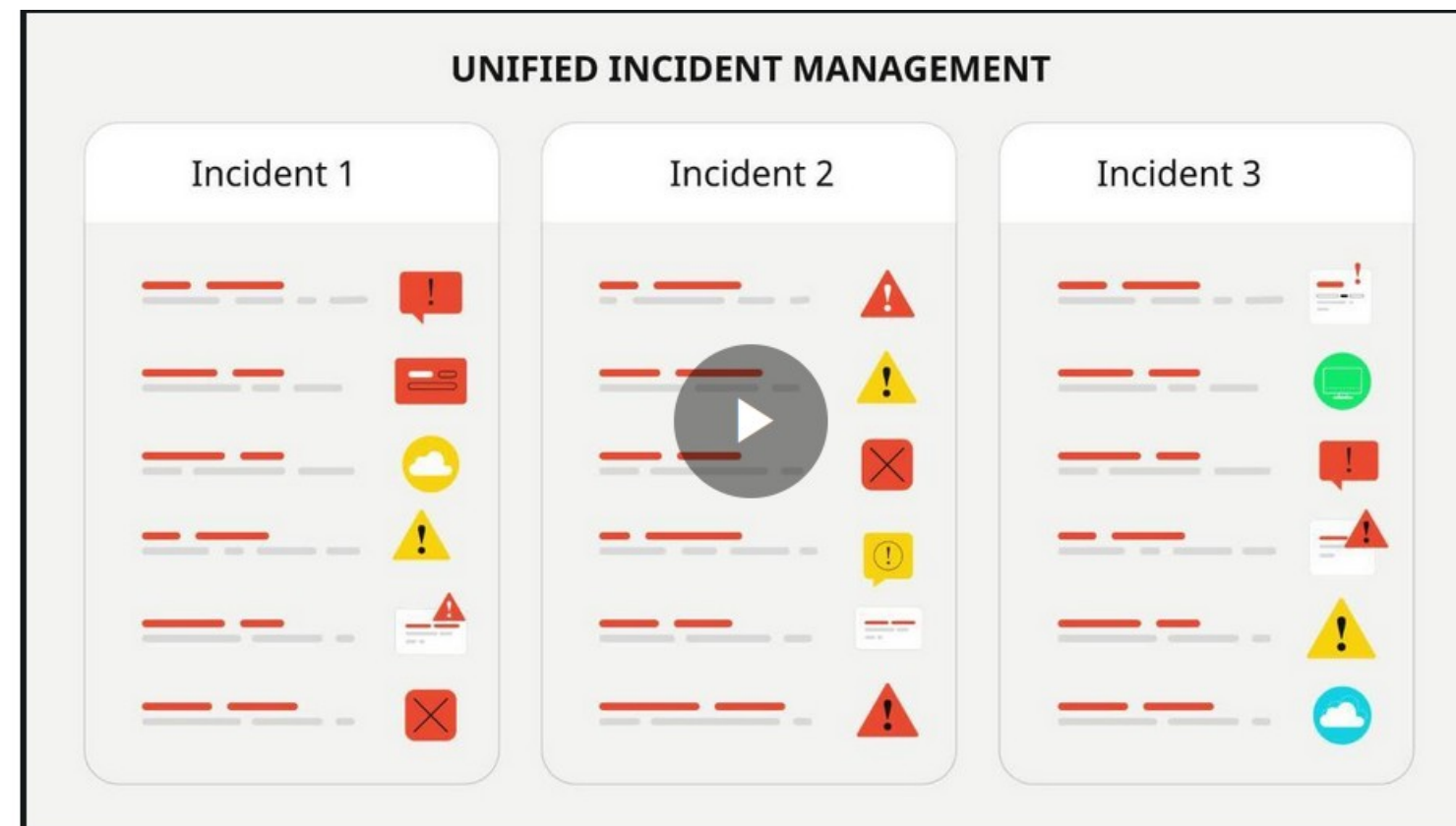


Ahora os toca a vosotros:

- Buscad 1 ejemplo de IOC
- Buscad otro ejemplo de IOA

XDR (Extended Detection and Response)

- Arquitectura que unifica datos de distintas herrrrramientas → En distintas capas
- Soluciona problemas de *visibilidad* entre herramientas
- Típicamente basado en la nube (SaaS)
- ¿XDR es un EDR *vitaminado*?



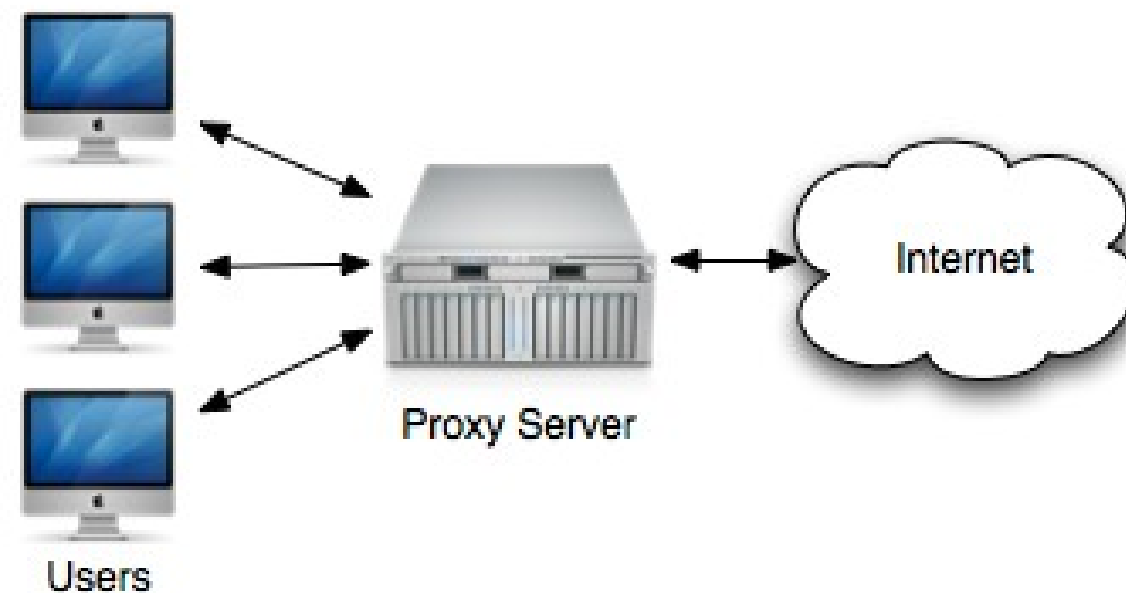
Firewall

- Dispositivo de seguridad de red
- Monitoriza conexiones y bloquea comunicaciones en base a unas reglas
- Puede ser hardware, software o ambos
- Premisa básica:
 - Tráfico proveniente de un entorno menos seguro ha de ser inspeccionado antes de ser permitido
- Históricamente 1º línea de seguridad de red
- Por sí sólo no cubre toda la seguridad de red pero es la *piedra de toque*



Proxy

- Pasarela de paso entre usuario e Internet
- Mediante un intermediario se impide el acceso directo de ciberatacantes a una red privada
- Se pueden utilizar como firewalls o filtro web
- También mejoran la disponibilidad → Balanceo de carga y memoria caché



VPN (Virtual Private Network)

- Famosas desde la implantación del teletrabajo en plena pandemia
- Importantes para todo tipo de empresas, grandes y PYMES
- Se establece una conexión *directa* entre un dispositivo de usuario y un servidor remoto → desde el ordenador del trabajador hasta la red de la empresa
- El ordenador obtendrá una IP rivada de la misma red de la empresa
- Conexión segura a través de una red MUY insegura (Internet) → ¿¿CÓMO?? → Cifrando toda informaciónl

Autenticación multifactor – MFA (Multifactor Authentication)

- Además de nuestras credenciales podemos proporcionar:
 - OTP (One-time password): Código generado periódicamente, aleatorio y de un solo uso
- Un tipo muy común de autenticación multifactor son los sistemas físicos o biométricos → ventajas e inconvenientes

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas ...	Artritis, reumatismo ...	Firmas fáciles o cambiantes	Ruido, resfriados ...

Autenticación multifactor – MFA (Multifactor Authentication)

- ¿¿Configuramos algún servicio a modo de ejemplo??

Cifrado de datos en equipos

- Para proteger información sensible/confidencial → cifrado de datos almacenados (incluidos dispositivos móviles)
- El cifrado deja ilegible la información para alguien sin la clave necesaria
- Clasificar tipo de información → decidir si necesita cifrado
- ¿Se deben cifrar las comunicaciones? Sí, por supuesto
- ¿Se deben cifrar los datos? Evidentemente
- ¿Los datos que están guardados dónde?
 - Todo dato sensible en dispositivos de almacenamiento, incluyendo las copias d seguridad
 - También se incluyen todos los dispositivos que se conecten a la red de nuestra empresa
- ¿Y los móviles? ¿Es que nadie piensa en los móviles?
 - Sí, tranquila Helen, a éstos deben añadirse medidas extra como **geolocalización**, **bloqueo remoto** o **borrado**

remoto

Análisis de vulnerabilidades

- Proceso para:
 - Detectar
 - Clasificar
 - Priorizar
- Deficiencias en nuestros sistemas y aplicaciones
- Se utilizan escáneres de vulnerabilidades → producto software → permiten automatizar el proceso
- Estos escáneres tienen varias formas de uso

Análisis de vulnerabilidades

Buenas prácticas:

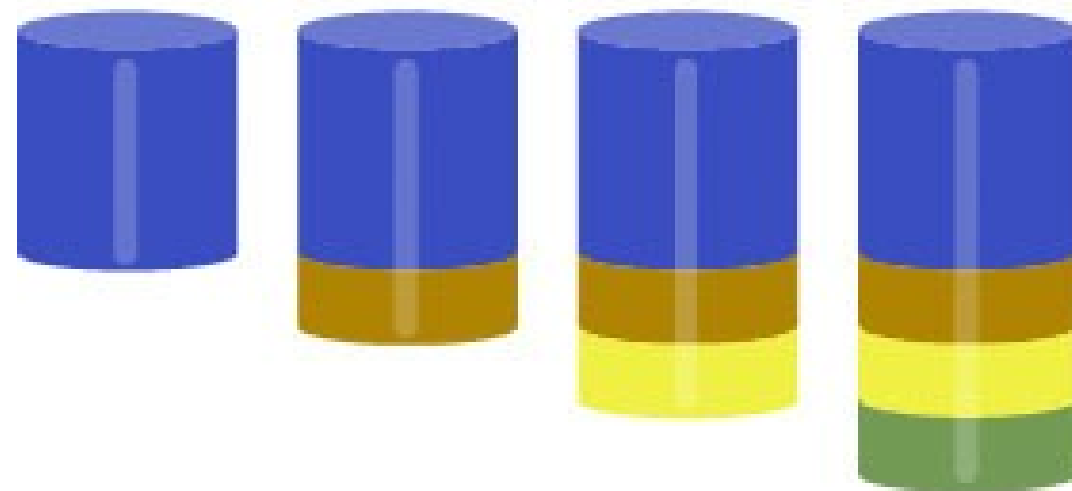
- Analizar todos los activos
- Escaneos periódicos regulares
- Asignar responsables
- Proceso de parcheo y/o corrección
- Generar informes

Backups (Copias de seguridad)

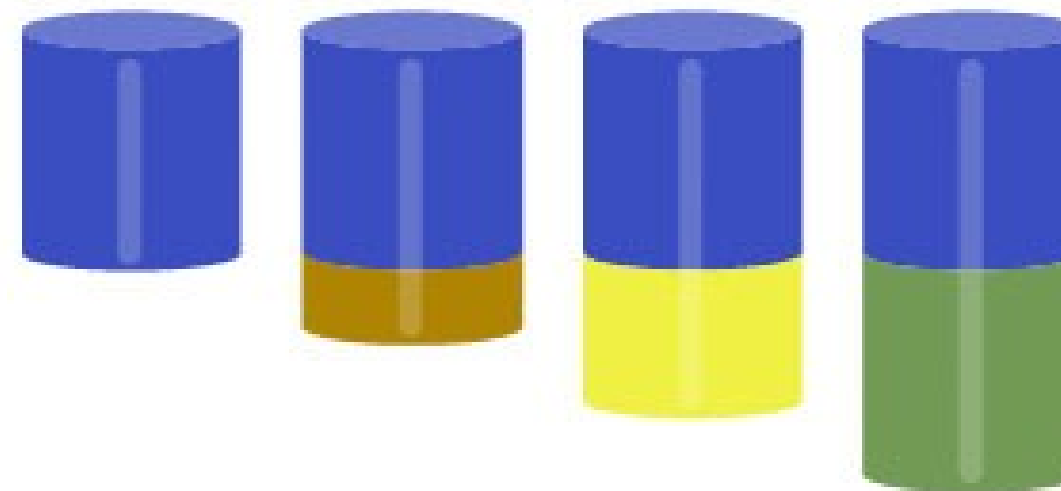
- Lo primero que ha de quedar claro es que **SON IMPRESCINDIBLES**.
- 3 tipos de copia:
 - Completa: incluye todo
 - Diferencial: incluye sólo lo que ha cambiado desde la última completa
 - Incremental: incluye lo que ha cambiado desde la última copia de seguridad, sea cual sea
- Para restaurar:
 - Última copia completa + las copias incrementales hasta la fecha del fallo

Backups (Copias de seguridad)

Backup incremental



Backup diferencial



- Backup completo
- Primer backup
- Segundo backup
- Tercer backup

BACKUP TOTAL - INCREMENTAL - DIFERENCIAL

Para el incremental requiere el respaldo completo mas todos los respaldos incrementales.
Para el diferencial requiere el respaldo completo y únicamente el último respaldo diferencial.

Backups (Copias de seguridad)

Comprobemos si ha quedado claro:

En general, la copia incremental:

- (a) Ocupa más que la copia completa.
- (b) Ocupa más que la copia diferencial.
- (c) Ocupa menos que la copia diferencial.

Backups (Copias de seguridad)

En general, la copia incremental:

- (a) Ocupa más que la copia completa.
- (b) Ocupa más que la copia diferencial.
- (c) **Ocupa menos que la copia diferencial.**

Backups (Copias de seguridad)

- Elegir entre diferencial o incremental para el backup diario depende de cada empresa y sus características:
 - Si hay poca actividad diaria → copia diferencial, porque aporta la ventaja de que cada copia diaria tiene toda la información necesaria para recuperar ese día
 - En el incremental, si perdemos la cinta de un día, puede que tenga ficheros que no estén en las copias siguientes
 - Si hay mucha actividad, estamos de nuevo ante el problema de mantener la consistencia de la copia.

Backups (Copias de seguridad)

- Estrategia 3-2-1:
 - 3 copias de datos
 - 2 formas almacenamiento distintas
 - 1 copia fuera de la empresa

¡MUY IMPORTANTE!

Hacer pruebas para corroborar que las copias se pueden restaurar correctamente y se mantiene la integridad

Ciberseguros

- Mismo concepto que un seguro tradicional
- “*Tercerizar*” el riesgo
- Aseguradora evalúa el nivel de seguridad de la empresa, exige medidas y ofrece un seguro
- Se incluyen cosas como por ejemplo:
 - Robo datos
 - Ataques DoS
 - Responsabilidad civil
- Un ciberseguro es un complemento **NO** una solución → medidas de seguridad propias
- Hoy en día se ofrecen cada vez menos ciberseguros o extremadamente caros

Formación a empleados

- Factor humano → eslabón más débil de la cadena
- Se pueden tener los sistemas más avanzados de seguridad pero... hay que fortificar el factor humano
 - Esta formación debe estar presente en TODOS los niveles de empleados
- La formación en materia de ciberseguridad NO es un coste, es UNA INVERSIÓN → largo plazo
- Puntos sobre los que se puede educar:
 - Identificación phishing
 - Navegación segura
 - Uso seguro contraseñas
 - Uso responsable móviles
 - Identificación ingeniería social

Formación a empleados

- Factor humano → eslabón más débil de la cadena
- Se pueden tener los sistemas más avanzados de seguridad pero... hay que fortificar el factor humano
 - Esta formación debe estar presente en TODOS los niveles de empleados
- La formación en materia de ciberseguridad NO es un coste, es UNA INVERSIÓN → largo plazo
- Puntos sobre los que se puede educar:
 - Identificación phishing
 - Navegación segura
 - Uso seguro contraseñas
 - Uso responsable móviles
 - Identificación ingeniería social
- La formación debe resultar atractiva y práctica de cara al empleado → sólo así resultará útil

Antispam/Antiphising

- Pueden ser software o hardware
- Sistemas que examinan los emails en busca de indicios maliciosos
- El usuario recibe el email tras un filtrado previo

Algunas acciones que se llevan a cabo en este filtrado:

- Emular la apertura del email en un sandbox
- Data Loss Prevention (DLP) → protección frente a exfiltración de datos
- Listas blancas/Listas negras de dominios



Soluciones basadas en la nube

- Si una empresa (PYME p.ej.) no posee la capacidad necesaria de montar infraestructura previa



- Se subcontratan servicios y se utilizan soluciones en la nube
 - Se delega la administración y gestión a técnicos especializados → forma parte servicio
- Soluciones y herramientas que se pueden ofrecer en esta modalidad:
 - Firewall
 - Antispam/antiphishing
 - Antivirus
 - Backups
 - Autenticación
 - Gestión disp. Móviles
 - Gobernanza

Pentest o test de intrusión

- Simulación de un ataque real a la infraestructura empresarial
- Objetivo: descubrir vulnerabilidades o deficiencias a las que ponerle solución lo antes posible
- Las personas que llevan a cabo este proceso son expertos en ciberseguridad y se denominan *hacker éticos*
- Este test debe llevarse a cabo siempre con permiso contractual donde se detalle cada punto del proceso

TIPOS DE PENTESTING

- 1) Caja blanca: los hackers cuentan con toda la información del sistema
- 2)Caja negra: los hackers no cuentan con ninguna información previa
- 3)Caja gris: se cuenta de partida con información parcial del sistema

Fases de un pentest

- (1) Recopilación y planificación: Definir objetivos y recolectar datos
 - (2) Análisis de vulnerabilidades: Análisis de la situación, detectar puntos de entrada y vectores de ataque
 - (3) Modelado de amenazas y explotación: Comprobar viabilidad de lo detectado en la fase anterior
 - (4) Elaboración de informes: Informe lo más preciso posible para el cliente, junto con soluciones propuestas
- además debe tener 2 partes, ejecutiva y técnica

Consideraciones legales de un pentest

- Para “cubrirse las espaldas” y evitar repercusiones indeseadas → todo bien detallado y concretado en un contrato
- En el contrato se especifica sin lugar a dudas:
 - ✓ Máquinas y sistemas que son propiedad de la empresa contratante
 - ✓ Alcance
 - ✓ Horario de realización de las pruebas
 - ✓ Técnicas y herramientas que se utilizarán
 - ✓ Cláusula de confidencialidad



Phishing “ético”

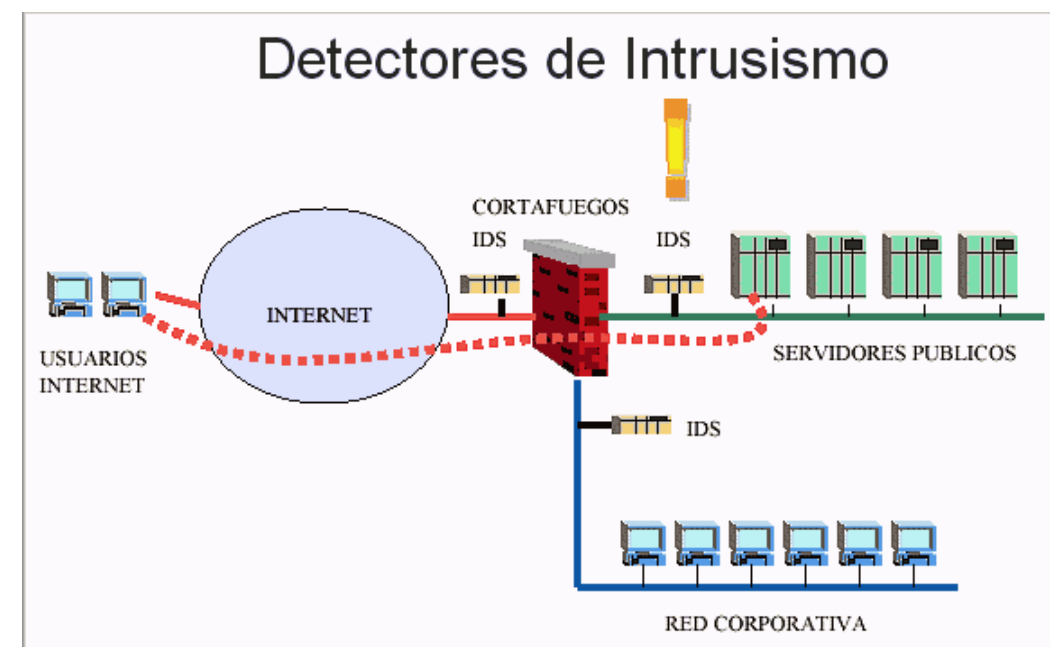
- Recordemos → factor humano es el eslabón más débil de la cadena + phishing es la mayor puerta de entrada de malware
- También comentamos anteriormente → Necesidad de formación en ciberseguridad a los empleados



- Todo ello justifica el ***phishing ético*** → campañas de phishing llevadas a cabo por la misma empresa

IDS (Intrusion Detection System)

- Sistemas monitorizar tráfico entrante → lo cotjean con una BBDD de firmas de ataque conocidas
- Actividad sospechosa → envían alerta al administrador → toman medidas oportunas
- Pueden ser ataques esporádicos (manuales) o periódicos (automáticos)
- Actuación reactiva → Detectan accesos sospechosos, no mitigan



¿Cómo funcionan los IDS?

- Existen dos **tipos** de IDS.

1) **NIDS (Network-based Intrusion Detection System)** → Monitorizan el tráfico de 2 formas:

- a) Todo el tráfico pasa a través de él
- b) Se hace una copia de todo el tráfico y se le envía

2) **HIDS (Host-based Intrusion Detection System)** → Comprueba actividad sospechosa sólo en un host, no en toda la red

¿Cómo funcionan los IDS?

- Típicamente se basan en 3 metodologías para detectar incidentes:
 - 1.Basada en firmas:** Se compara la unidad de actividad actual con una lista de firmas → así se distingue entre uso normal del PC vs uso fraudulento
 - 2.Detección basada en anomalías:** compara la definición de “actividad normal” con los eventos observados para detectar desviaciones
 - 3.Análisis de protocolos de estado:** utiliza información sobre las conexiones, manteniendo un registro de las mismas → busca cambios repentinos o bruscos en la actividad de red

IPS (Intrusion Prevention System)

- Software dedicado a la prevención de intrusiones → obviamente, carácter **preventivo**
- Sistemas que llevan a cabo un análisis en tiempo real de las conexiones → identifican ataques, anomalías, comportamientos sospechosos...



- Muchos proveedores ofrecen productos mixtos, llamándolos IPS/IDS, integrándose frecuentemente con cortafuegos y UTM (en inglés Unified Threat Management o Gestión Unificada de Amenazas)

Limitaciones de los IDS/IPS

- Están limitados a detectar únicamente ataques conocidos
- Generan **falsos positivos** (detectar una actividad legítima como anómala) → Dependientes de reglas que escribamos o carguemos
- Muy limitados ante el tráfico cifrado
- Visibilidad limitada en función del lugar de la red empresarial donde se coloquen

SIEM (Security Information and Event Management)

- Utilizado para monitorizar los ataques o peligros a los que nuestro sistema puede estar expuesto en ese momento.
- Es una plataforma de unificación de logs (registros) de todos los dispositivos de la red



¡Además es capaz de correlacionar los eventos que aparecen en ellos!



Capaz de detectar comportamientos anómalos o inusuales que puedan ser un indicio de ataque

MARCOS DE GESTIÓN

Para la prevención, protección, respuesta y gobierno

Comencemos...



Introducción

- Los marcos o *frameworks* de seguridad se basan en controles
- Nos permiten organizar nuestras actividades de ciberseguridad
- Los controles nos permiten llegar a un estado de madurez en ciberseguridad que
hayamos puesto como objetivo de antemano
- Ofrecen confianza

Tipos de marcos

- 1) Marcos de control
- 2) Marcos programáticos
- 3) Marcos de riesgo

Marcos de control

Se utilizan para:

- Desarrollar estrategias básicas de seguridad
- Ofrecer un conjunto de controles básicos
- Evaluar el estado actual
- Priorizar los controles a implementar

Marcos de control → NIST SP 800-53

- NIST: Instituto Nacional de Normas y Tecnologías de los EEUU
- Estándares y directrices para seguridad de la información
- Famosos servicios en la nube como Azure, AWS o GCP cumplen este estándar
- 20 familias distintas de controles
- Lista completa de controles

Visión general del NIST 800-53

- Catálogo integral de controles de seguridad y privacidad
- Familias → Controles → Refuerzo de los controles
- Podemos decidir cómo implementar controles en función de prioridad o de su impacto en el negocio

AC-18 WIRELESS ACCESS

Overview

Number	Title	Impact	Priority	Subject Area
AC-18	Wireless Access	LOW	P1	Access Control

Instructions

The organization:

AC-18a.

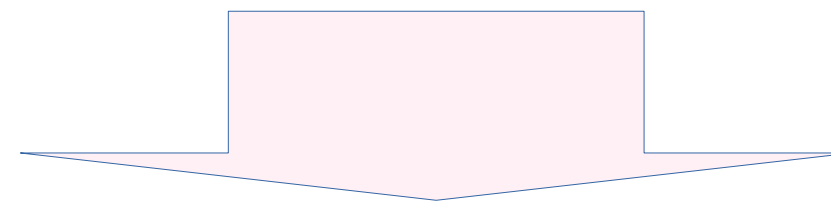
Establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access; and

AC-18b.

Authorizes wireless access to the information system prior to allowing such connections.

Controles CIS

- Raramente se implementarán todos los controles del NIST 800-53
- CIS (The Center for Internet Security) es una organización sin ánimo de lucro
- Comprometida con la creación de herramientas y soluciones de seguridad gratuitas
- Ofrece una colección de 20 controles prioritarios de ciberseguridad para reducir al máximo la superficie de ataque



Gran tasa de éxito

Controles CIS

- Pensado para organizaciones con recursos limitados → se les ofrece pautas básicas para una protección efectiva
- ¿Se pueden mapear estos controles CIS a otros controles de otros marcos de ciberseguridad?



- De hecho algunos sitios incluso se han tomado la molestia de hacer este mapeo por nosotros, ahorrándonos mucho tiempo, como por ejemplo:

Auditscripts

Marcos programáticos

- Ayudan con la comunicación a alto nivel con la capa ejecutiva de la empresa → mejorar perspectiva de la ciberseguridad
- Puntos clave:
 - Evalua estado ciberseguridad
 - Crear programa integral ciberseguridad
 - Medir seguridad del programa/análisis competitivo
 - Simplificar comunicación

Visión general de la serie 27000

- ISO (International Organization for Standardization) → Entidad que publica estándares internacionales de todo tipo
- La serie 27000 está dedicada a la seguridad de la información
- 27001 → Define plan de seguridad, requerimientos del ISMS (Information Security Management System)
- 27002 → Guía para la implementación de los controles de seguridad en una organización (encaminado a cumplir con la 27001 o no)

ISO 27001

- Define áreas de actuación → construir plan de seguridad y su estructura



 **pirani**

ISO 27001

- No suele aplicarse en EEUU → MUY exigente en recurso para aplicarse
- Sin embargo, todos los proveedores cloud la cumplen → ¿Por qué? → negocio internacional
- Los controles a implementar → Anexo A de la ISO 27001

ISO 27001

Los controles se distribuyen en estas 14 secciones:

- Políticas de seguridad de la información: A. 5.
- Organización de la seguridad de la información: A.6.
- Seguridad de los recursos humanos: A. 7.
- Gestión de Activos: A.8.
- Controles de acceso: A.9.
- Criptografía – Cifrado y gestión de claves: A.10.
- Seguridad física y ambiental: A.11.
- Seguridad operacional: A.12.
- Seguridad de las comunicaciones: A.13.
- Adquisición, desarrollo y mantenimiento del sistema: A.14.
- Gestión de incidentes de seguridad de la información A.16.
- Cumplimiento: A. 8.

NIST Cybersecurity Framework (CSF)

- Framework más sencillo → permite comunicarse de forma simple con personal no técnico a propósito de las funciones y controles a implementar
- Responde a preguntas de la empresa tales como:
 - ¿Qué estamos haciendo a día de hoy?
 - ¿Cómo lo estamos haciendo?
 - ¿A dónde queremos llegar?
 - ¿Cuándo queremos llegar?
- Básicamente → guiar a empresas a gestionar y reducir riesgos → mejores prácticas
- Este marco se compone de 3 partes:
 1. Marco básico (Framework **Core**)
 2. Niveles de implementación (Framework Implementation **Tiers**)
 3. Perfiles del marco (Framework **Profiles**)

Nucleo básico (core)

- Conjunto de:
 - 1) Actividades
 - 2) Resultados a obtener
 - 3) Referencias informativas

Perfiles

- El core sirve como guía para desarrollar los perfiles en la organización
- Los perfiles identifican el estado actual y el estado objetivo en cuanto a ciberseguridad en la empresa
- Nos sirven para ver la brecha que debemos cubrir si queremos cumplir con las metas marcadas sobre gestión de riesgos, estableciendo así una hoja de ruta

Niveles de implementación (Tiers)

- Define la visión de una organización en cuanto a riesgos de ciberseguridad y como de maduros son los procesos que se implementan → desde lo más forma hasta lo más informal

NIST CSF

- Volviendo una vez más al **core** del CSF → 5 funciones clave, de alto nivel de abstracción:
 - 1) Identificar: Inventariar activos, roles, responsabilidades
 - 2) Proteger: Medidas de seguridad adecuadas
 - 3) Detectar: Acciones para monitorizar e identificar eventos/incidencias seguridad
 - 4) Responder: Capacidad actuación frente a un incidente seguridad
 - 5) Recuperar: Identifica las acciones para recuperarse de un incidente
- El propio NIST nos pone a disposición un archivo Excel para la implementación del CSF

Incluso se incluye un mapeo de cada subcategoría a otros marcos, como el NIST 800-53 o los controles CIS (CSC)

“Hueco” o vacío en la función de identificación
(Gobernanza y evaluación de riesgos)

Marcos de riesgo

- Cuando la organización es madura en cuanto a ciberseguridad → subir un escalón en nuestro plan de seguridad
- Estos marcos ayudan a:
 - Definir claves evaluar y gestionar riesgo
 - Estructura programa gestión riesgo
 - Identificar, medir, cuantificar el riesgo
 - Priorizar actividades

Marcos de riesgo - Ejemplos

- Podemos hablar de dos tipos de estándares dentro de este tipo de frameworks:

1) Gestión de riesgos:

- NIST SP 800-39: Gestión de riesgos
- NIST SP 800-37: Gestión de riesgos en sistemas info federales (RMF)

2) Evaluación/valoración de riesgos:

- NIST SP 800-30: Evaluación de riesgos

RMF

- A pesar de estar dirigido a organizaciones federales → útil porque trata la gestión de riesgos y eso debe abordarse en toda organización
- Consta de **6 fases**

ISO 27005

- Es la encargada de abordar el tema de la gestión del riesgo en los stmas. de información
- Define un enfoque sistemático para la gestión de riesgos
- Aquí un diagrama con la metodología → Muy parecido al NIST 800-30

¡SORPRESA!

- Aparecen dos *cajones* al respecto de tratamiento del riesgo y aceptación del riesgo



Modelo FAIR

- Estos frameworks miden el riesgo de forma **cualitativa** (LOW, MEDIUM, HIGH)
- El modelo FAIR introduce la medición **cuantitativa** → aporta una metodología
- Compatible con todos los marcos de riesgo anteriores
- A alto nivel, para entendernos:

Riesgo = Impacto x Probabilidad (de ocurrencia)

Riesgo = Impacto x (Vulnerabilidad x Amenaza)

Mitre Framework

- MITRE ATT&CK → MITRE Adversarial Tactics, Techniques, and Common Knowledge
- Base de datos de conocimiento sobre la metodología usada por grupos de ciberdelinquentes
- Sabiendo las técnicas y tácticas que usan, podremos defendernos adecuadamente

Gobernanza de datos

- Gobernanza de datos → Es un concepto que habla del correcto tratamiento y gestión de los datos empresariales.
- Concepto clave para la transformación digital en las empresas
- Marco de gobernanza de datos resulta esencial → Big Data
- 4 pilares básicos:

1) Gobernanza

2) Gestión

3) Calidad

4) Seguridad y privacidad

Pautas a considerar para un buen gobierno del dato según la UNE y resumidas por el Ministerio de asuntos económicos

Conclusiones

- A medida que el plan de seguridad de nuestra organización madura → iremos eligiendo implementar al menos uno de los marcos de cada tipo
- Recordar:
 - 1) Marcos de control → Identifican controles a implementar
 - 2) Marcos programáticos → Ayudan a construir plan integral de seguridad y mejorar la comunicación con la parte no técnica
 - 3) Marcos de riesgo → Priorizar tareas de seguridad apropiadamente

Dudas, preguntas, ruegos, aclaraciones, inquietudes, curiosidades...



¡Adiós!