Institución Universitaria

Acreditación Institucional ITM
"Juntos trabajando para llegar a la meta"

FACULTAD DE INGENIERÍAS

"Ingeniería para la transformación social con equidad y conciencia ambiental"

Institución Universitaria

Gestión de riesgos

Héctor Fernando Vargas Montoya
Msc. Seguridad de las TIC
Oficina L304- Fraternidad
hectorvargas@itm.edu.co

Normas de Convivencia

- Horario
  - Sábado 10:00 am – 1:00 pm
  - Agosto 3 – 16 Noviembre (16 semanas)
- Pausas activas – 10 min.
  - 11:30 a.m.
- Se espera una participación activa/colaborativa
- Tener presente el uso de celulares u otros dispositivos.

Institución Universitaria

AGENDA

Módulo 1:

1. Introducción a la gestión de riesgos
2. Terminología de riesgos
3. Riesgos lógicos de las TIC
    1. Ataques y vulnerabilidades técnicas
4. Factores de riesgos.

Héctor Fernando Vargas Montoya

AGENDA

Módulo 2: Gestión de riesgos ISO 27005

- Introducción y definición: Marco conceptual
  - Clasificación y valoración de activos de activos
- Variables de medición para probabilidad e impacto
- Identificación de amenazas y calificación del riesgo.
- Generación de mapas de riesgos.

Héctor Fernando Vargas Montoya

Institución Universitaria

AGENDA

Módulo 3: Mitigación de riesgos

- **Controles: lógicos y físicos, administrativos y culturales.**
- **Herramientas de prevención y detección.**
- **Pruebas de intrusión y Ethical Hacking**
- **Controles legales: Condiciones de Uso, cláusulas contractuales y Delitos informáticos.**
- **Cierre del ciclo de riesgos: Revisión del GAP y pruebas de cierre.**
- **Medición** de la Eficacia en los controles
- **ROSI: Retorno a la inversión de seguridad.**

Héctor Fernando Vargas Montoya

Evaluaciones

Eventos evaluativos	Ponderación (%)	Fecha
Ensayo: La ciberseguridad y la industria 4.0	20	12 Agosto
Trabajo: Gestión de Riesgos. Objetivo: Crear un mapa de riesgos sobre un caso de estudios, con sus respectivos análisis.	30	21 Septiembre
Entrega 1: Levantamiento de activos y clasificación de éstos.	10	7 septiembre
Entrega 2: Mapa de riesgos	20	21 Septiembre
Trabajo y exposición: Mapa de riesgos de proyectos tecnológicos Objetivo: Ejecutar un análisis de riesgos sobre un proyecto dentro del caso de estudio o el proyecto de la maestría.	20	12 Octubre
Trabajo final: Análisis de riesgos técnico + controles. Objetivo: Crear un mapa de riesgos teniendo como fuente un análisis de vulnerabilidades técnico, así como establecer una estrategia de controles y monitoreo para los riesgos técnicos.	30	16 Noviembre

Competencia

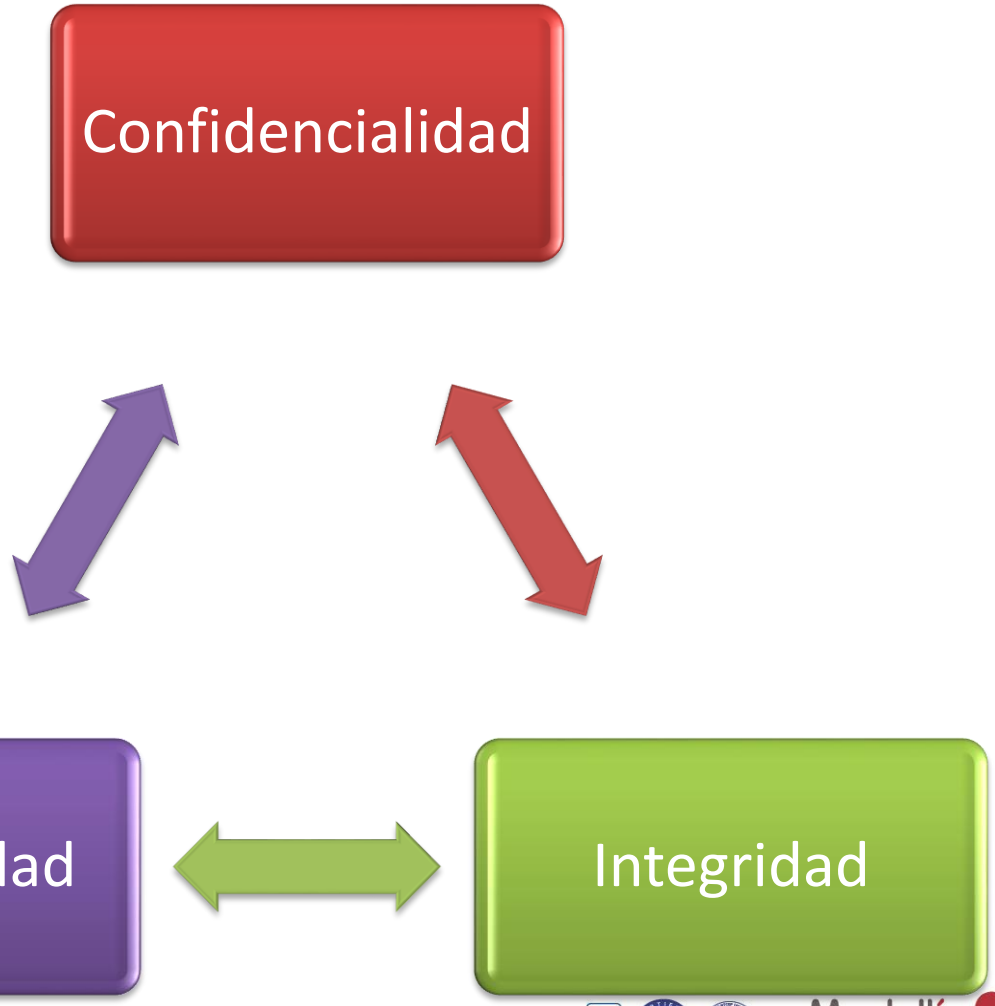
Elaborar el análisis de riesgos de seguridad de la información con base en el inventario obtenido de activos de información, las vulnerabilidades en los sistemas y las amenazas que pueden tener incidencia sobre los procesos organizacionales de la compañía.

Institución Universitaria

INTRODUCCIÓN GENERAL

Héctor Fernando Vargas Montoya

¿Que protege la seguridad?

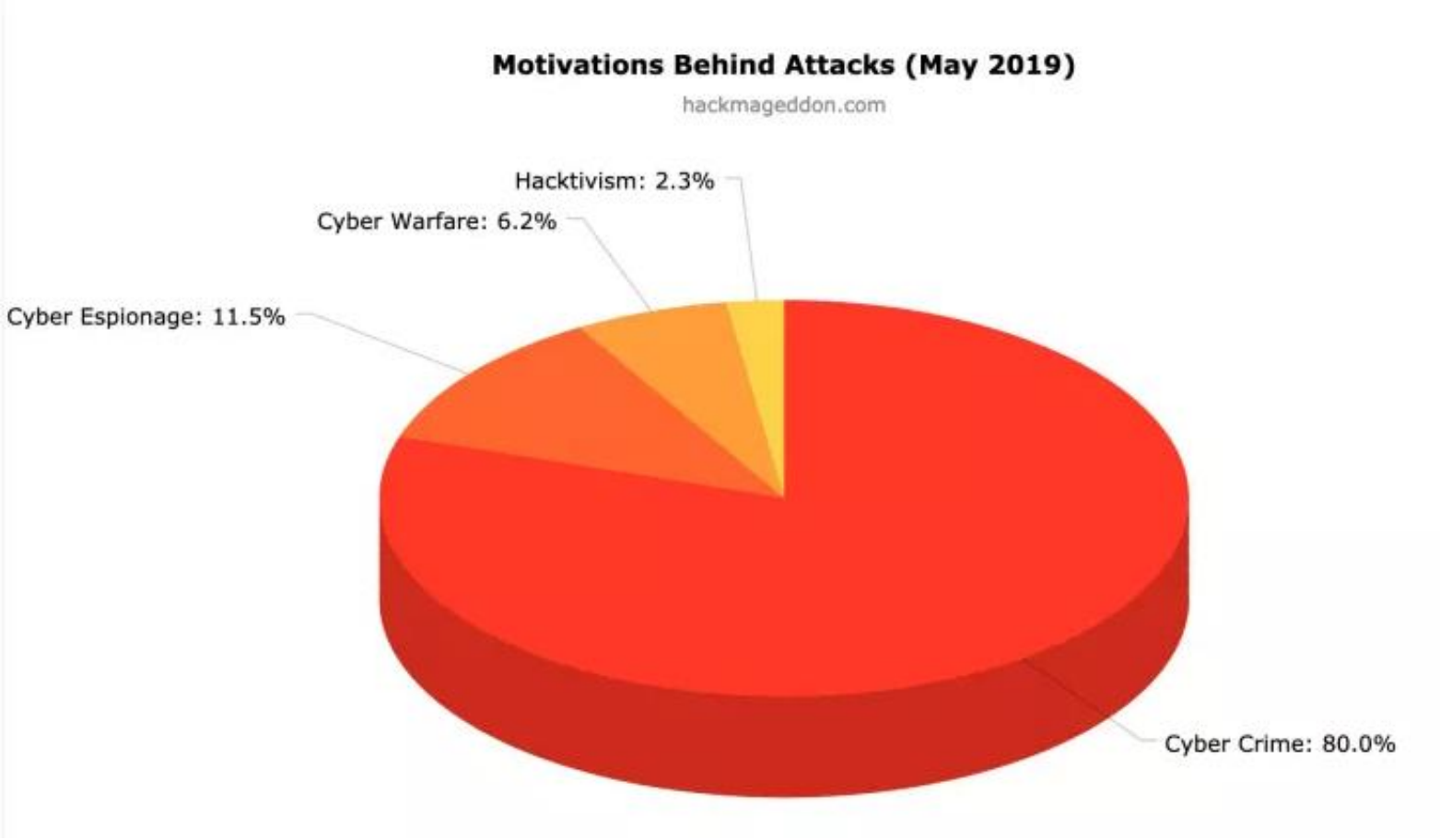


Héctor Fernando Vargas Montoya

Algunos datos

Tomado: ACIS 2019- https://acis.org.co/archivos/Revista/Sistemasedicion151.pdf

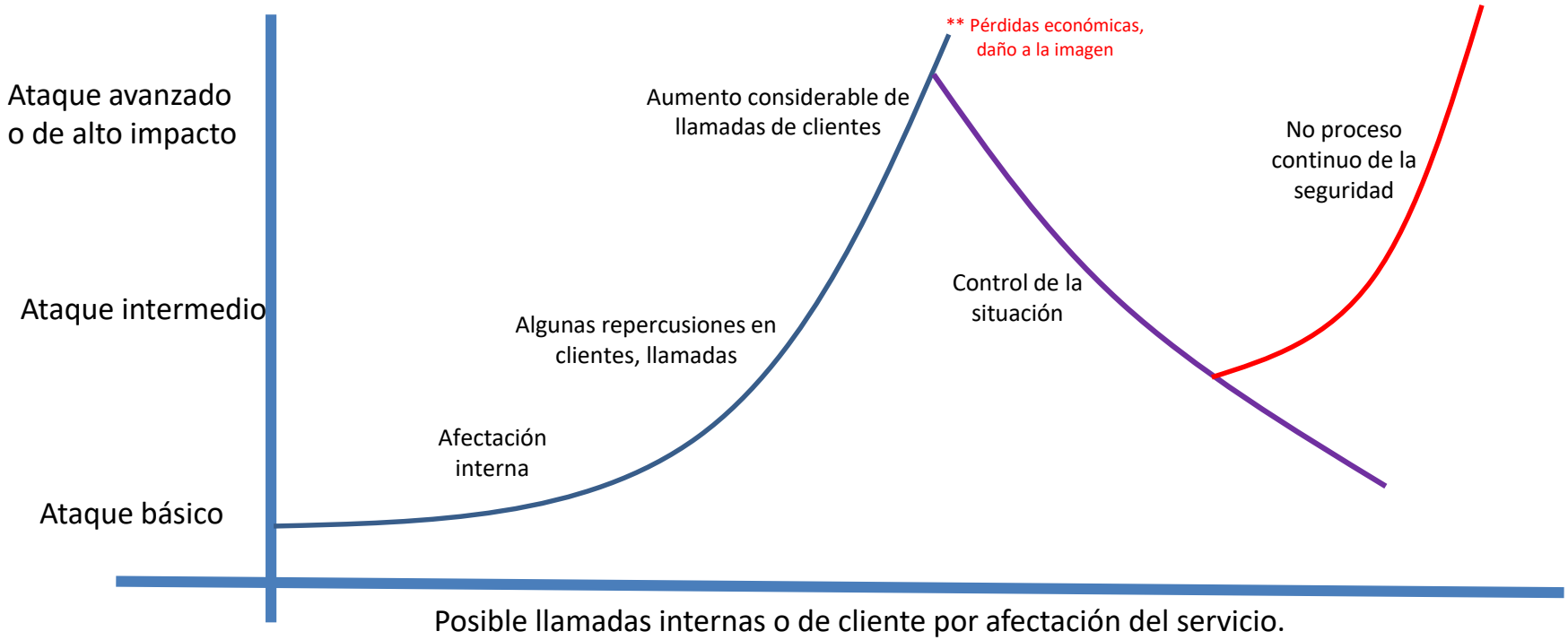
Algunos datos



https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

Institución Universitaria

Afectación de la seguridad en el servicio



Fuente propia

Institución Universitaria

RIESGOS

Héctor Fernando Vargas Montoya

GESTIÓN DE RIESGOS

La administración de riesgos una estructuración de elementos, estrategias y procesos para manejar la incertidumbre que es relativa a las amenazas y vulnerabilidades en los activos y sistemas, la cual se ejecuta a través de actividades secuenciales que incluye la identificación, evaluación del riesgo, manejo y mitigación.

Factores de riesgos

Un factor de riesgo es una agrupación de eventos, elementos o circunstancias con similares características.

Héctor Fernando Vargas Montoya

Factores de riesgos

Naturales/Ambientales

- Son riesgos propios de la naturaleza o medio ambiente

Tecnológicas:

- Se derivan del peligro originado por una inadecuada interacción del ser humano con el desarrollo tecnológico

Humano:

- Asociados a la persona

Estratégicas, Administrativas y Financieros:

- Toma de decisiones y administración general de las organizaciones

Socio-culturales:

- Fenómenos impactados por la sociedad o a la cultura en general

Proyectos:

- Asociados de la ejecución de los proyectos

Biológicos ó Bioriesgo:

- Factor asociados con la presencia de organismos o sustancias derivadas de estos

Tecnologías de información y comunicaciones:

- Se derivan de la utilización de la infraestructura tecnológica y sus componentes (programas informáticos, elementos de redes y comunicaciones, sistemas de información y aplicaciones)

Institución Universitaria

Elemento de aprendizaje

Del caso de estudio, revise cuales factores de impacto pueden aplicar a éste y cuales pueden ser de mayor afectación según su criterio.

Acorde al factor de impacto, ¿puede haber información relevante?

Héctor Fernando Vargas Montoya

Elemento de aprendizaje

- QUE ES UNA VULNERABILIDAD TÉCNICA?
- QUE ES UNA AMENAZA INFORMÁTICA?
- QUE ES UN RIESGO?
- ¿Cuál ES LA DIFERENCIA ENTE FRECUENCIA Y PROBABILIDAD DEL RIESGOS?
- INDIQUE AL MENOS 10 AMENAZAS TECNOLÓGICAS

GESTIÓN DE RIESGOS

¿Que es una vulnerabilidad?

Exposición a un riesgo, debilidad, fallo o hueco de seguridad detectado en alguna organización, proceso, procedimiento, programa o sistema informático.

GESTIÓN DE RIESGOS

Activo

Son los recursos del sistema de seguridad de la información necesarios para que una organización logre sus objetivos.

GESTIÓN DE RIESGOS

¿Que es una amenaza?

- Cualquier situación, evento o ente con potencial de daño, que pueda presentarse en un sistema.
- Fuente de daño potencial o una situación que cause pérdidas.

Ejemplos

- **Programa malicioso.**
- **Incendio.**
- **Hurto**
- **Espionaje**
- **Suplantación**
- **Black-Hat Hacker**

GESTIÓN DE RIESGOS

Frecuencia

Es una medida sobre la rata de ocurrencia de un evento expresado por el número de ocurrencias de un evento en un tiempo dado.

Probabilidad

La probabilidad de un evento específico o resultado, medido por el coeficiente de eventos o resultados específicos en relación a la cantidad total de posibles eventos o resultados, expresada en porcentaje.

GESTIÓN DE RIESGOS

Institución Universitaria

Frecuencia y probabilidad

La siguiente tabla resume la cantidad de eventos de ataques informáticos a un gremio de empresas:

Mes	Cantidad
Dic/2019	15
Enero/2019	14
Febrero/2019	8
Marzo/2019	30
Abril/2019	20
mayo/2019	18

Cual es la frecuencia mensual de los eventos y cual es la probabilidad de que ocurra en el siguiente mes, en los siguientes 2 meses, en los 6 meses siguientes?

FRECUENCIA: 105/6 = 17.5 eventos por mes

PROBABILIDAD – 1 mes: 17.5/105 = 16.66% que ocurra
PROBABILIDAD – 2 mes: 35/105 = 33.33%
PROBABILIDAD – 5 meses: 87.5/105=83.33%

Que es un RIESGO?

Es un hecho potencial, que en el evento de ocurrir puede impactar negativamente la seguridad, los costos, la programación o el alcance de un proceso de negocio o de un proyecto.

La posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se lo mide en términos de consecuencias y probabilidades, cuando una AMENAZA explota o aprovecha una VULNERABILIDAD.

Que es un RIESGO?

Riesgo residual

El nivel restante de riesgo luego de tomar medidas de tratamiento del riesgo.

ELEMENTO DE APRENDIZAJE

Identificar cada elemento si es un activo, una amenaza, vulnerabilidad.

Ítem	activo	amenaza	vulnerabilidad
Servicio DHCP			
Red inalámbrica			
Arduino			
Apache versión 2.2			
Falta de proveedor clave			
Puerto 135 abierto			
Puerta del IDC defectuoso			
Password craking			
Ransomware			
Ausencia de Firewall			
IPS			
WAF			
Protocolo SSL 3.0 activo.			
Sistemas de almacenamiento sin contraseñas			
Información			

PROPIEDADES DE LOS RIESGOS

- Tiene la posibilidad de que ocurra, pero no hay certeza.
- Es algo que potencialmente es **perjudicial**, no es necesariamente beneficioso o neutro.
- Es algo que con el tiempo puede crecer, decrecer, desaparecer ó concretarse.

Causa

Motivo, razón o circunstancia por la cual se genera algo (en esta caso, un riesgo).

Agente generador

Todas aquellas personas, cosas, eventos, acciones o circunstancias que tiene la capacitad de generar un riesgo.

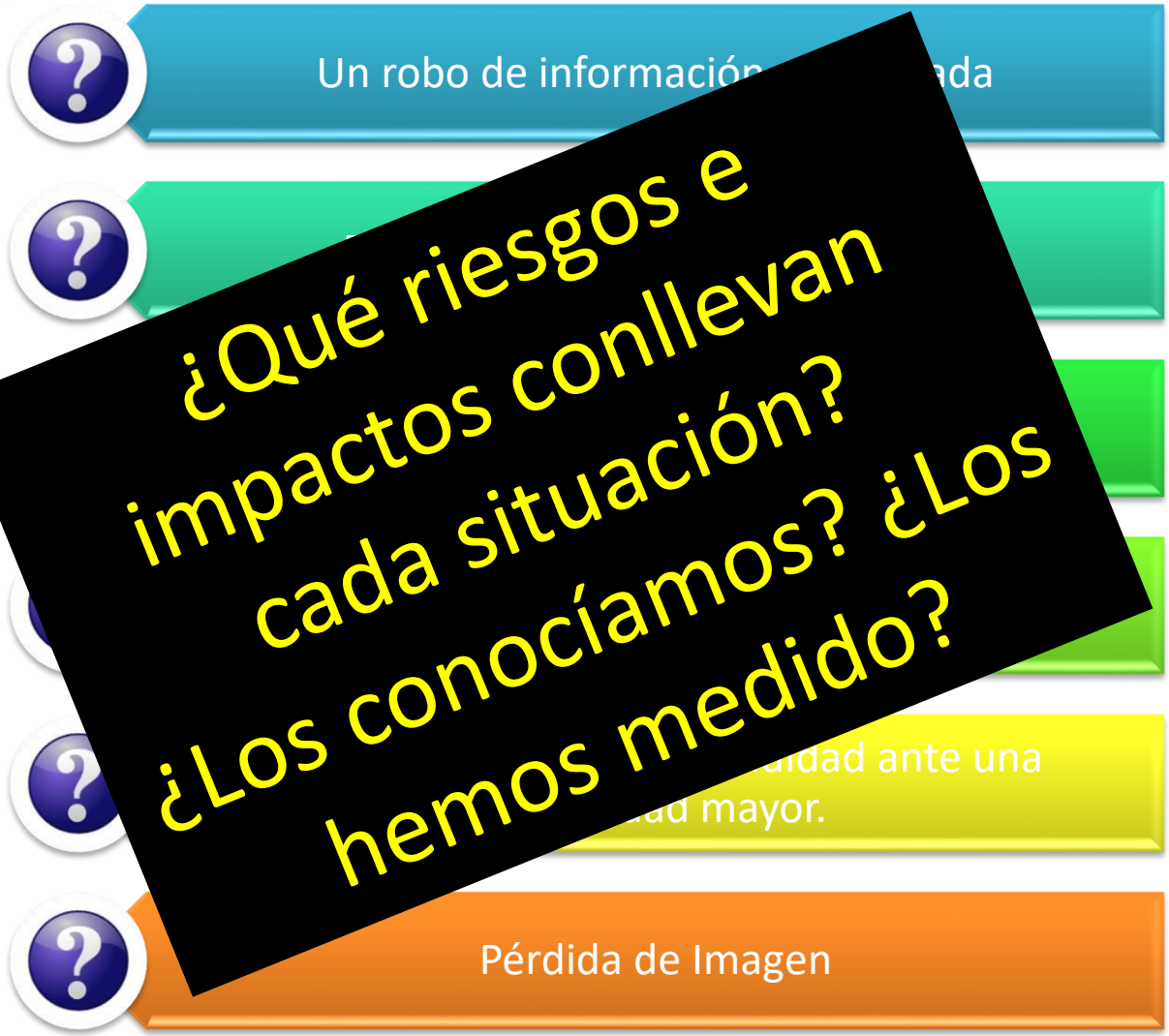
Consecuencia ó efecto

Es el producto de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia.

Qué tan preparados estamos para:

- Un robo de información privilegiada
- Robo continuo de cajas menores.
- Identificar una suplantación de identidad.
- Identificar y controlar un ataque informático.
- Ejecutar un plan de continuidad ante una adversidad mayor.
- Pérdida de Imagen

Qué tan preparados estamos para:



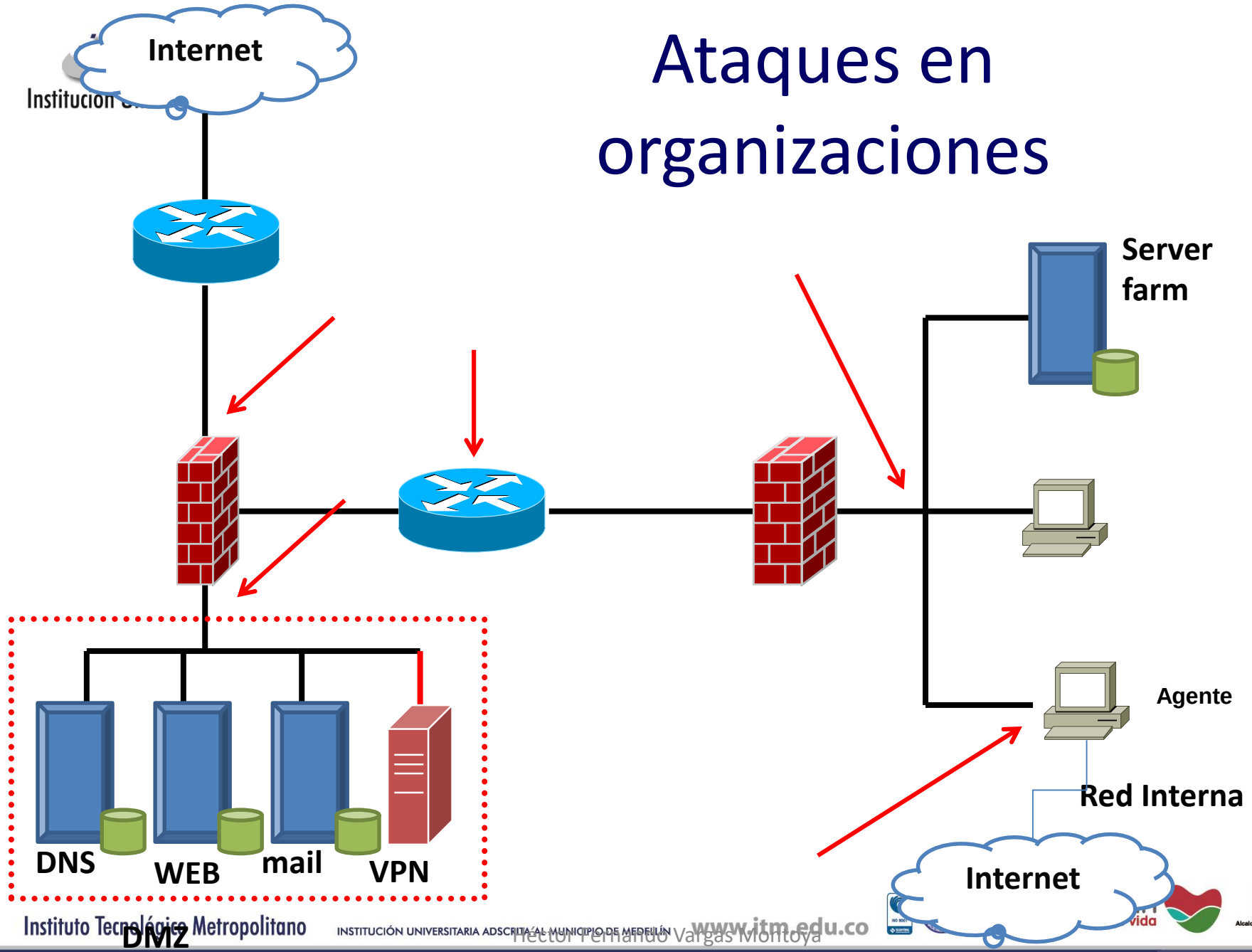
¿Qué riesgos e impactos conllevan cada situación? ¿Los conocíamos? ¿Los hemos medido?

AMENAZAS Y ATAQUES

Que es un ATAQUE?

Acción ofensiva de algo o alguien, que, superando las barreras de seguridad establecidas van por un bien común: Dañar, extraer, ver o modificar algo.

Ataques en organizaciones



AMENAZAS Y ATAQUES

Institución Universitaria

ATACANTE

Persona, dispositivo o elemento software capaz de ejecutar un ataque.

- Black hat Hacker
- White hat Hacker
- Grey hat hacker

ELEMENTO DE APRENDIZAJE

Para los siguientes riesgos indique las posibles causas, agente generadores, ataques y efectos o impactos si se materializa el riesgos.

1) Cifrado de información por código malicioso.
2) MItM.
3) Robo de información confidencial desde la base de datos.
4) Phishing en el servidor Web
5) Alto procesamiento en el servidor de aplicaciones (indisponibilidad).

AMENAZAS Y ATAQUES

Institución Universitaria

ATACANTE

Persona, dispositivo o elemento software capaz de ejecutar un ataque.

Newbie

- Principiante

Phreaker

- Busca fallas en los sistemas de telecomunicaciones

Lammer

- Se creen “hackers”

Cómo se ejecuta un ataque

1. Técnicas de footprints y enumeration

   - ✓ Nombres de dominios
   - ✓ Bloques de IP’s
   - ✓ Direcciones IP de servidores específicos
   - ✓ Puertos y servicios usados
   - ✓ Meta-busquedas en redes sociales
   - ✓ Información remanente en sitios Web
   - ✓ Errores involuntarios
   - ✓ Google hacking

Cómo se ejecuta un ataque

2- Manipular usuarios para ganar acceso

- Ingeniería Social
  - Dumpster Diving
  - Ingeniería social inversa: Se crea el problema y luego se llama para dar la solución
  - Hacerse pasar por familiar
- Password Cracking
  - En diccionarios: propios o comunes
  - Fuerza bruta: combinación y permutación.
  - Híbridos
- Phishing
- Spam – cadenas en redes sociales

Cómo se ejecuta un ataque

3. Escalar privilegios

- ✓ Subir a una cuenta que “deje hacer más”.
- ✓ Revisar información del sistema
- ✓ Lanzar un malware (trojan horse, exploit, etc)

4. Recolectar contraseñas

- ✓ Obtener otras cuentas de usuario
- ✓ Cuentas que pueden llegar a otros sistemas/puntos de la red

Cómo se ejecuta un ataque

- Instalar back doors y/o port redirectors
  - Garantizar acceso al sistema hackeado
  - Usualmente difícil de detectar

- **TOMAR VENTAJA DEL SISTEMA COMPROMETIDO**
  - USARLO COMO PUENTE PARA OTROS SISTEMAS
  - REPETIR LOS PASOS ANTERIORES EN CADA SISTEMA
  - MANTENER LA DISPONIBILIDAD DEL SISTEMA

Elemento de aprendizaje

- Haga uso de varias técnicas de footprint para obtener información de un sitio web:
  - búsqueda en dns-whois
  - google hacking

EN GOOGLE:

- PASSWORD INURL “NOMBRE URL“
- "INDEX OF" / "CHAT/LOGS“

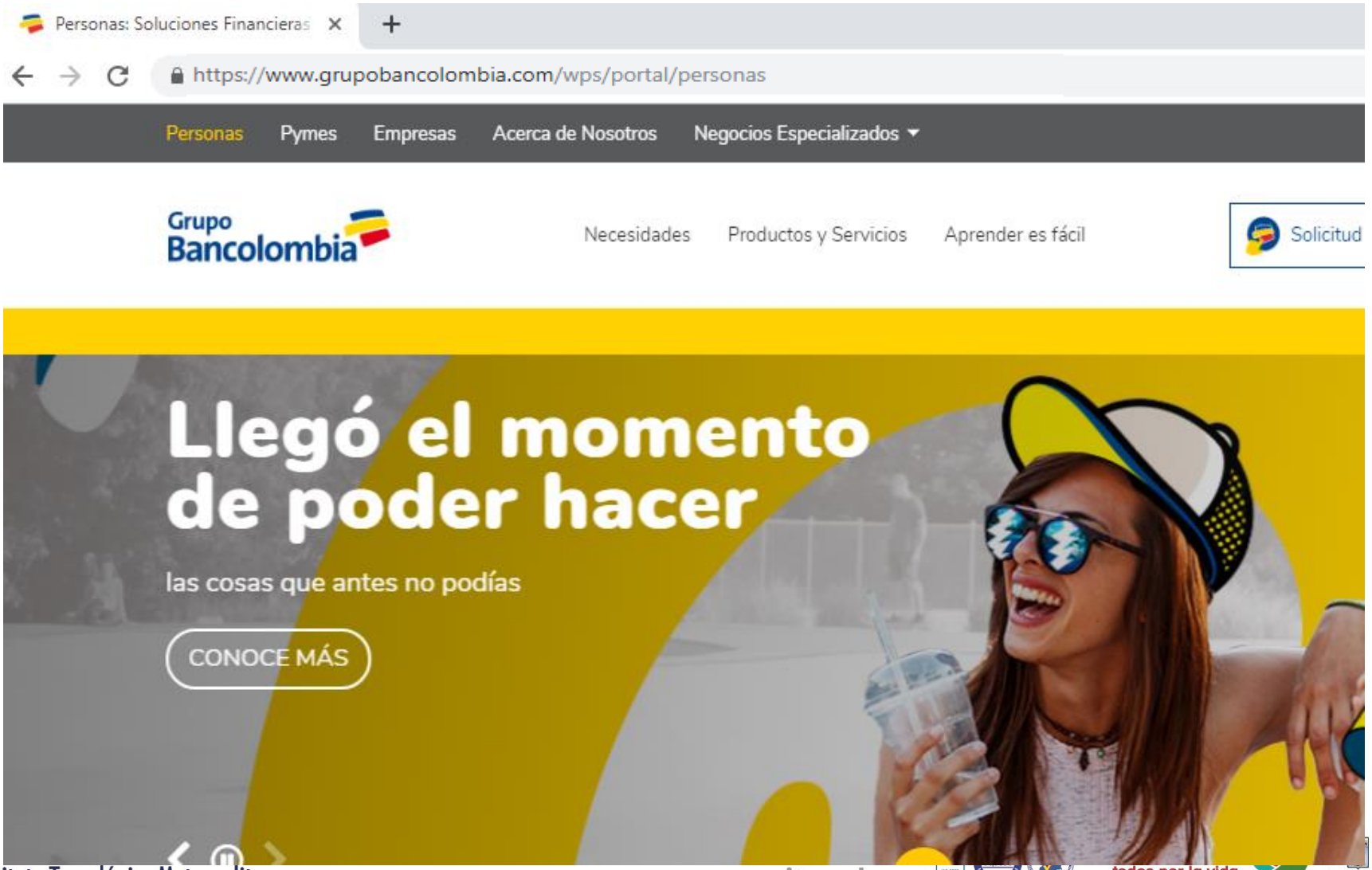
- https://www.exploit-db.com/google-hacking-database
- https://wifibit.com/google-hacking/

ALGUNOS PROGRAMAS Y UTILIDADES

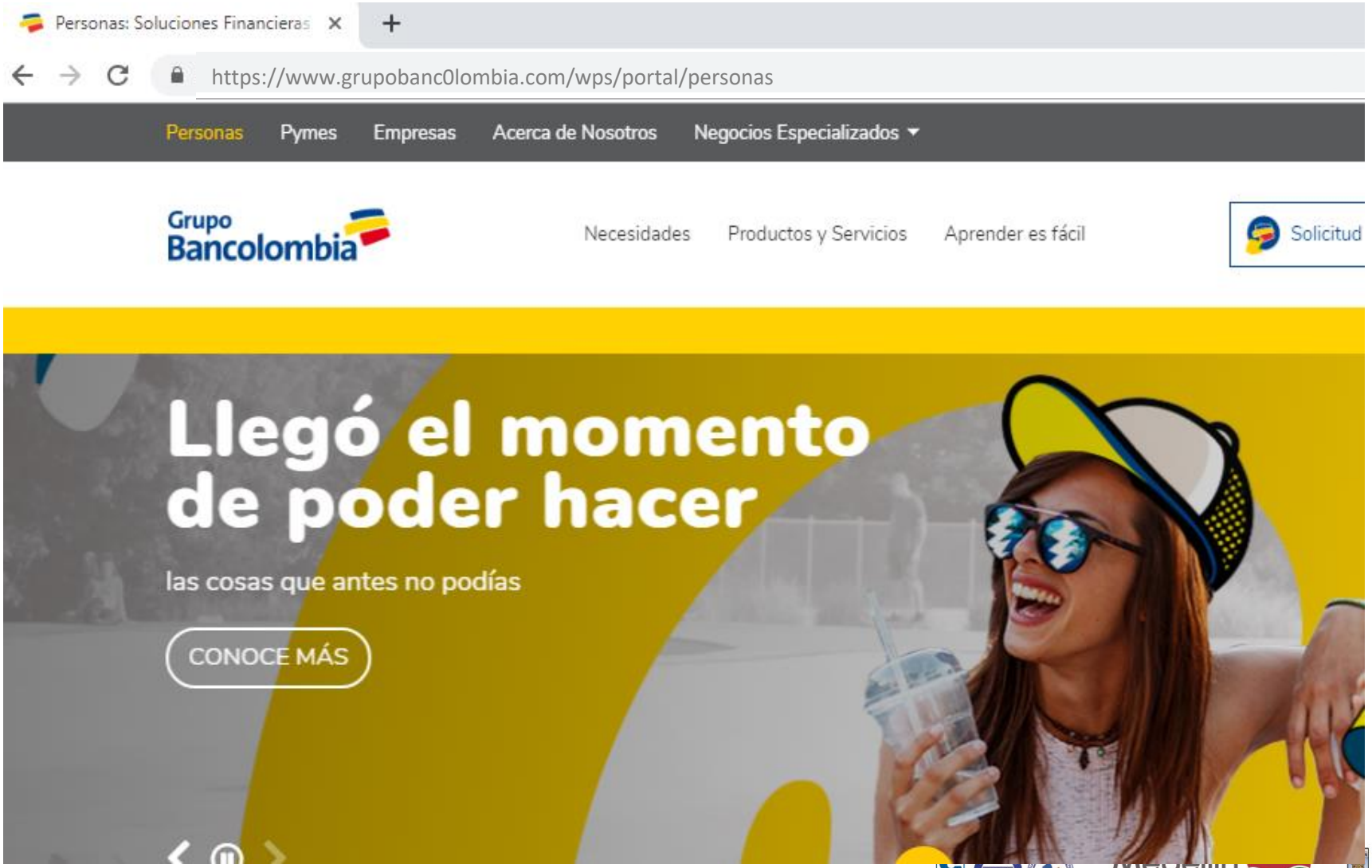
- **Nslookup, whois, mxtool box, traceroute (tracert)**
- **Nbtstat**
- **Nmap:** Network Mapper. Port Scanner
- **Foundstone ScanLine:** Port scanner.
- **Nessus:** Analizador de vulnerabilidades
- **Metasploit:** Generador y motor para explotar vulnerabilidades
- **FOCA** Fingerprinting Organizations with Collected Archives

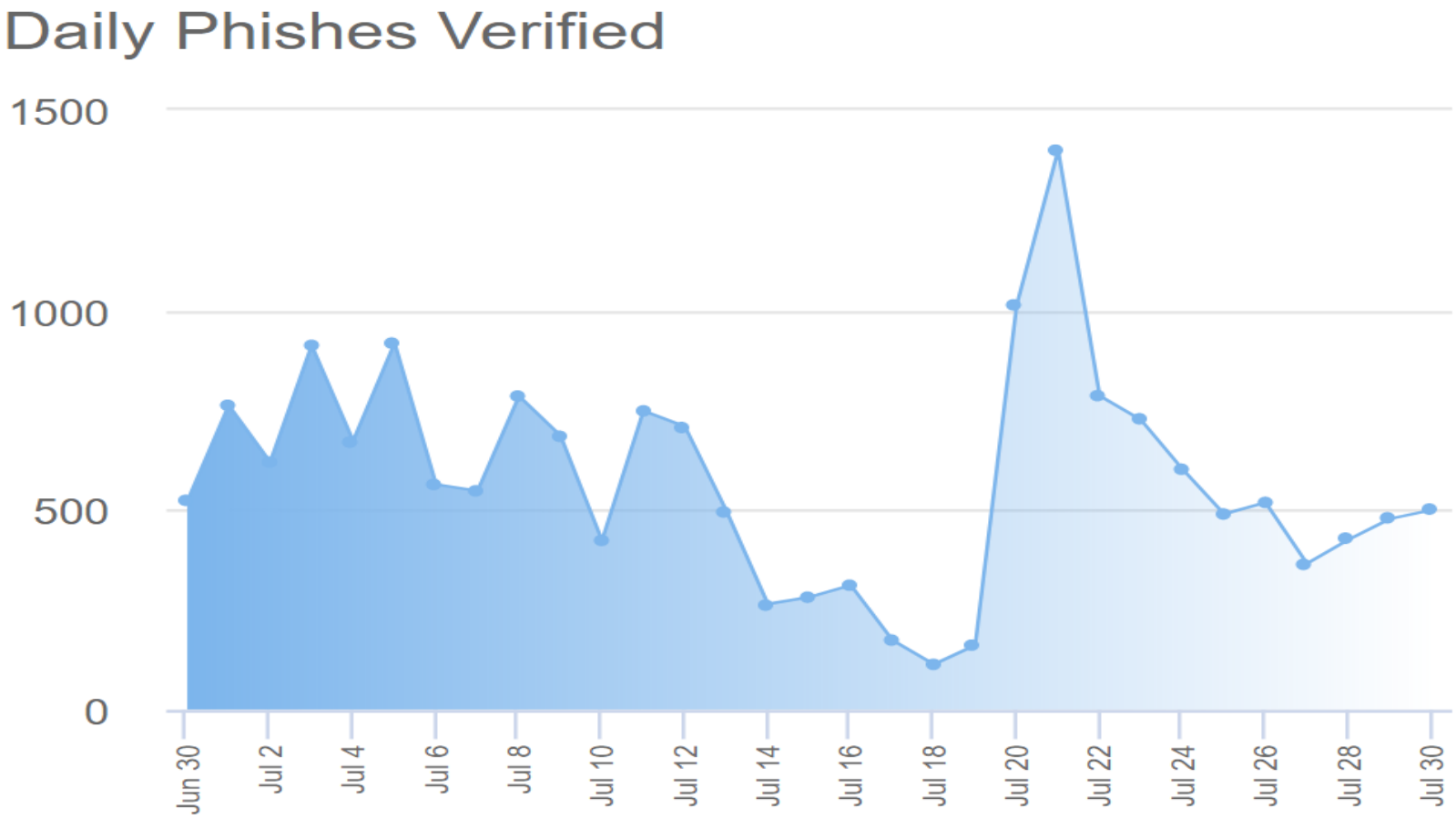
Malware (Código Malicioso)

- *Del ingles **mal**icious soft**ware***
- *Tienen como objetivo infiltrarse en las redes y computadores con el fin de dañar, extraer, copiar y/o modificar datos, programas, archivos y/o parámetros del sistema.*
- El término malware comprende virus, gusanos, troyanos, rootkits, spyware, adware, crimeware, etc.
- Algunos de estos son casi imposibles de detectar (rootkit).


Personas: Soluciones Financieras
https://www.grupobancolombia.com/wps/portal/personas
Personas
Pymes
Empresas
Acerca de Nosotros
Negocios Especializados
Grupo Bancolombia
Necesidades
Productos y Servicios
Aprender es fácil
Solicitud
Llegó el momento de poder hacer
las cosas que antes no podías
CONOCE MÁS

¿Notaron algo diferente?


Personas: Soluciones Financieras
https://www.grupobanc0lombia.com/wps/portal/personas
Personas
Pymes
Empresas
Acerca de Nosotros
Negocios Especializados
Grupo Bancolombia
Necesidades
Productos y Servicios
Aprender es fácil
Solicitud
Llegó el momento de poder hacer
las cosas que antes no podías
CONOCE MÁS



http://www.phishtank.com/

Institución Universitaria

Vectores de ataque

Mecanismo usado por un atacante para descubrir y/o explotar una vulnerabilidad

Hacia Juegos Online	Phishing	Autenticación y autorización
IoT	Intrusión en redes	Monedas virtuales
Estafas en redes sociales	Escaneo de redes y servicios	Control de acceso y cifrado
Malware	S.O y software	Aplicaciones Web y servicios

Institución Universitaria

Ataques a las redes y sistemas

- ARP poisoning
- scanning
- tcp syn attack
- SQL injection
- deface
- cross-site scripting
- acceso no autorizado
- shoulder surfing
- buffer overflow
- spam
- PhishingCaptura de código IMSI - International Mobile Subscriber Identity
- Esteganografía
- Estafas nigerianas
  - Clásica, lotería, animales regalados, compra de vehículos, ebay, Empleos, romance

- DNS amplification
- Suplantación
- Cadenas de correo
- Spoofing: de MAC, IP, ARP o cualquier servicio.
- PASSWORD CRAKING
- Dumpster Diving
- Ingeniería social
- Exploit
- Fragment Flood y Jumbo Frame
- The man in the middle
- Forward de correo
- Jamming o flooding
- BlueSnarfing
- Robo de datos desde los móviles.
- Robo de credenciales Móviles

Elemento de aprendizaje

Para los siguientes elementos tecnológicos, indique qué posibles ataques puede sufrir:

Switch	
Portal Web en Apache	
Red Microsoft	
Sistema LDAP	
Servicio Correo	
Smartphone con Android	
Personas	
Router con el NTP activo.	

Qué es DoS/DDoS

Un ataque de negación de servicio (Denied of service, por sus siglas en ingles) es un ataque que causa que un servicio o sistema este por fuera o no pueda brindar un servicio determinado a los usuarios y equipos legítimos.

Da indisponibilidad a los sistemas, afectando uno de los pilares fundamentales de la seguridad

Qué es DoS - Denied of service

El ataque DoS entonces, da indisponibilidad a los sistemas por un tiempo determinado a través de:

- Consumos excesivos de anchos de banda.
- Deshabilitar servicios que son requeridos por el sistema operativo.
- Superar la capacidad de algún buffer, el cual ya no podrá entregar la información respectiva.
- Aumentar el nivel de procesamiento de la CPU y almacenando información adicional en cantidades en la memoria RAM

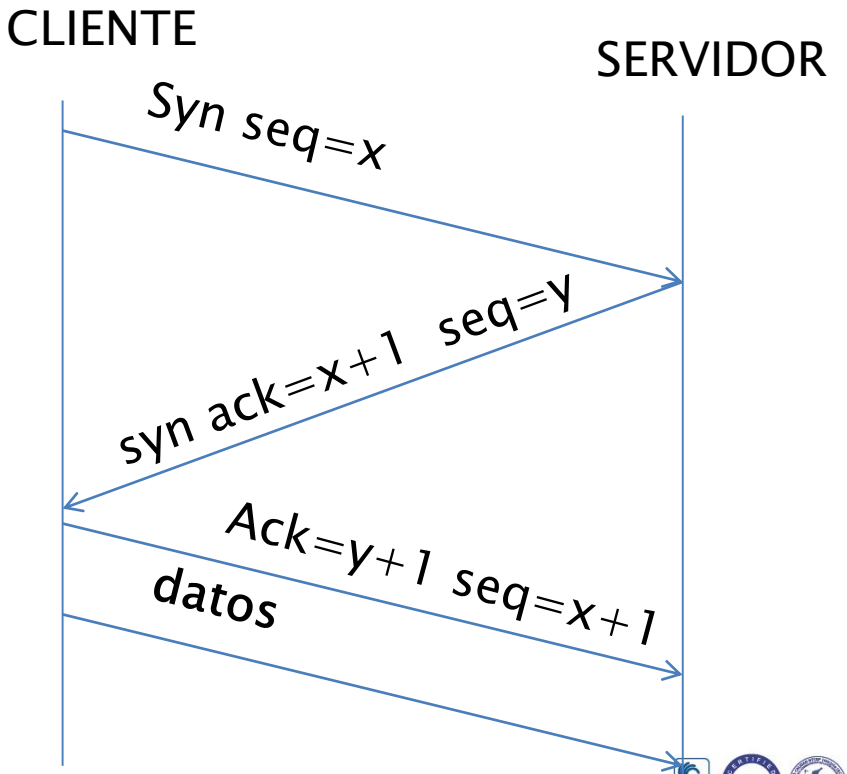
Pruebas de estrés

Sin embargo esta técnica de ataque puede servir para realizar pruebas y comprobaciones de capacidad y realizar así un rediseño de capacidad. Se trata de pruebas de estrés o de capacidad, que le permite a las personas comprender y entender la capacidad real de un dispositivo determinado.

Tipos de ataques conocidos

- **SYN Flood**

Paquete TCP



Ataques Slowloris

- Solicitudes GET o POST solo del encabezado, manteniendo los socket de los servidores saturados.
  - Sockstress
  - TCH-SSL-DoS
  - R.U.D.Y (Are-You-Dead-Yet).

ATAQUES/VULNERABILIDAD *BASES DE DATOS*

- Conexiones no autorizadas a través de ODBC – Open database Conectivity ó JDBC
- Conexiones no autorizadas con herramientas Ad-Hoc
- Envenenamiento de XML
- Versiones obsoletas de compilación
- Activación sin control de elementos ADO – ActiveX data Object.
- No encriptación de OLTP – Online Transaction Processing.
- ABRAZOS MORTALES: Minería de datos, consultas extensas en bases de datos.

Redes inalámbricas

No es posible limitar las conexiones.

- La configuración del propio servidor (punto de acceso mal configurados).
- La escucha (pinchar la comunicación del envío de datos). Aunque depende de la configuración del servidor, es posible interceptar.
- El sistema de cifrado (WEP, Wireless Equivalent Privacy). Si se utiliza un cifrado menor de 128 bits, es posible factorizar el código de cifrado en unas horas con computadores suficientemente potentes.
- Hacking a WPA y WPA2
- MiTM

ELEMENTO DE APRENDIZAJE

Identificar cada ejemplo qué tipo de ataque puede ser.

Comportamiento	Posible Ataque
El servidor Web envía un mensaje de *Not found*	
El servidor de archivos no permite más conexiones.	
El router no responde	
El sitio Web muestra información de otra empresa	
El tráfico del Firewall tiene más ancho de banda de lo normal.	
Mi Smartphone se ha consumido todos los datos.	
Dirección IP duplicada en la red	

Fuentes de información sobre vulnerabilidades.

http://nvd.nist.gov/

BugtraqID
http://www.securityfocus.com/vulnerabilities

Elemento de aprendizaje

De las fuentes de vulnerabilidades, consulte para las siguientes tecnologías:

- Windows server 2016
- Cisco
- Oracle
- MongoDB
- Joomla
- Php
- Java
- Linux Redhat

Elemento de aprendizaje

Segú la percepción. ¿Qué plataforma tecnológica considera usted con más vulnerabilidades?

Windows - Linux

Elemento de aprendizaje

Ver:

http://zone-h.org

Vulnerabilidades por proveedor entre marzo y agosto de 2018

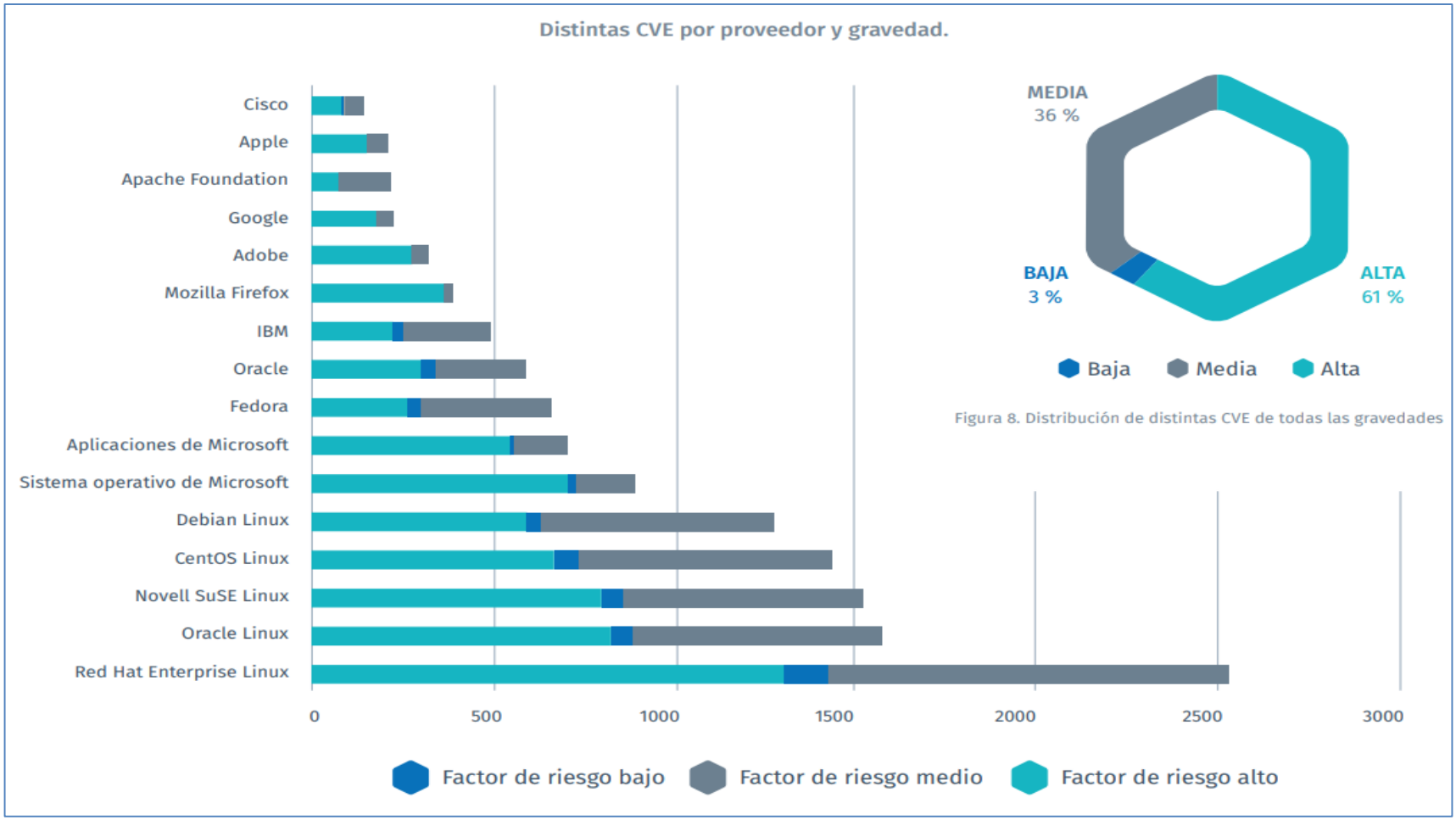


Figura 8. Distribución de distintas CVE de todas las gravedades

http://es-la-static.tenable.com/translations/en/Vulnerability_Intelligence_Report-ENG.pdf

http://www.flu-project.com/p/herramientas-de-seguridad.html

Footprinting y Fingerprinting: búsqueda de información

1. Anubis (Web oficial: http://flu-project.blogspot.com.es/p/herramientas-de-flu-project.html)
2. Maltego (Web oficial: http://www.paterva.com/web5/)
3. Nslookup (Información: http://es.wikipedia.org/wiki/Nslookup)
4. Dig (Información: http://en.wikipedia.org/wiki/Dig_%28Command%29)
5. Visualroute (Programa: http://visualroute.visualware.com/)
6. Whois (Programa: http://www.whois.net/)
7. Nsauditor (Web oficial: http://www.nsauditor.com/)
8. Foca (Programa: http://elevenpaths.com/lab_foca.html)
9. Httprint (Web oficial: http://www.net-square.com/httprint/)
10. Ldap Browser (Programa: http://www.ldapbrowser.com/)
11. Archieve.org (Web oficial: www.archieve.org)
12. Yougetsignal (Web oficial: www.yougetsignal.com)
13. Netcraft.com (Web oficial: www.netcraft.com)
14. Dnsstuff (Web oficial: www.dnsstuff.com)
15. Wfuzz (Información y programa: http://www.edge-security.com/wfuzz.php)
16. Nmap (Programa: http://nmap.org/download.html)
17. Zenmap (Interfaz gráfica de Nmap http://nmap.org/zenmap/)
18. Shodan (Información y servicio: http://www.shodanhq.com/)
19. Unicorn Scan (Información y programa: http://www.unicornscan.org/)

Aplicaciones para descargar webs

1. HTTrack (http://www.httrack.com/)
2. FileStream Web Boomerang (http://www.filestream.com/webboomerang/)
3. Website Ripper Copier (http://www.tensons.com/products/websiterippercopier/)

Escáneres de vulnerabilidades

1. GFI (Web oficial: http://www.gfi.com/languard/)
2. MBSA (Web oficial: http://technet.microsoft.com/es-es/security/cc184924.aspx)
3. SSS (Programa: http://www.safety-lab.com/en/products/securityscanner.htm)
4. WIKTO (Programa: http://www.baxware.com/wikto.htm)
5. ACUNETIX (Web oficial: http://www.acunetix.com/)
6. NESSUS (Web oficial: http://www.nessus.org/nessus/)
7. OpenVAS (Escaner de vulnerabilidades libre derivado de Nessus: http://www.openvas.org/)
8. RETINA (Información y programa: http://www.global-tools.com/retina.htm)
9. WEBCRUISER (Información y programa: http://sec4app.com)
10. NIKTO (Información y programa: http://cirt.net/nikto2)
11. FLUNYMOUS (Escáner de vulnerabilidades para Wordpress y Moodle: http://www.flu-project.com/download
12. WP-SCAN (Información y programa: http://code.google.com/p/wpscan/)

Exploits

1. Metasploit (Web oficial:http://www.metasploit.com/)
2. WinAUTOPWN (Programa: http://24.138.163.182/quaker/v2/w/winAUTOPWN_2.5.RAR)
3. Exploit-DB [Base de datos de exploits] (http://www.exploit-db.com/)

http://www.flu-project.com/p/herramientas-de-seguridad.html

Institución Universitaria

Malware

1. FLU - (Troyano Open Source): (http://www.flu-project.com)
2. Hacker defender (Tutorial (rootkit): http://foro.elhacker.net/hacking_avanzado...html)
3. Netcat (Tutorial: http://foro.elhacker.net/tutoriales...html)
4. Crypcat (Programa: http://sourceforge.net/projects/cryptcat/)
5. Rootkit Revealer (Programa: http://sysinternals-rootkitrevealer.softonic.com/)
6. AVG AntiRootkit 1.0.0.13 (Programa: http://www.grisoft.cz/79461)
7. Ice Sword (Programa: http://icesword.softonic.com/)
8. Fu.exe (Rootkit: http://www.wisedatasecurity.com/herramientas/FU_Rootkit.zip)
9. Ikklogger 0.1 (Keylogger http://foro.elhacker.net/....html)
10. File Mon (Programa: http://technet.microsoft.com/es-es/sysinternals/bb896642.aspx)
11. Kgb Spy (Programa beta (troyano): http://kgb-spy-keylogger.softonic.com/)
12. Subseven (Troyano: http://www.vsantivirus.com/sub722.htm)

Distribuciones de Linux orientas a auditoría

1. Wifislax (Página oficial: www.wifislax.com)
2. Wifiway (Página oficial: www.wifiway.org)
3. Backtrack (Página oficial: www.backtrack-linux.org)
4. Samurai (Página oficial: http://sourceforge.net/projects/samurai/)
5. Helix (Página oficial: http://www.e-fense.com/h3-enterprise.php)
6. Caine (Página oficial: http://www.caine-live.net/)
7. Bugtraq (Página oficial: http://www.bugtraq-team.com)

http://www.flu-project.com/p/herramientas-de-seguridad.html

Institución Universitaria

¿Preguntas?