Universidad de Buenos Aires
Facultad de Ciencias Económicas

Ataques Cibernéticos

Material de Estudio

Traducción y Comentarios

ATAQUES CIBERNÉTICOS MASIVOS

(*Massive Cyber Attacks*)

A continuación se presenta la traducción y organización conceptual de los ataques mostrados en la imagen, explicados desde la perspectiva de la gestión de Tecnologías de la Información (TI) y orientados a estudiantes de administración.

1️⃣ Ataques contra la Disponibilidad de los Sistemas

🔷 Ataque DDoS

DDoS (Distributed Denial of Service / Denegación de Servicio Distribuida)

Consiste en saturar un servidor, red o aplicación con un volumen masivo de tráfico proveniente de múltiples equipos comprometidos, impidiendo que los usuarios legítimos accedan al servicio.

Impacto organizacional:

- Caída de sitios web.
- Interrupción de plataformas de e-commerce.
- Pérdida de ingresos y reputación.

Elementos de TI a considerar:

- Balanceadores de carga.
- Firewalls avanzados.
- Sistemas anti-DDoS.
- Arquitecturas escalables en la nube.

2️⃣ Ataques contra la Confidencialidad

🔷 Phishing

Intento de engaño mediante correos electrónicos, mensajes o sitios falsos para obtener credenciales o información sensible.

Impacto organizacional:

- Robo de credenciales.
- Fraude financiero.
- Acceso indebido a sistemas internos.

Elementos de TI a considerar:

- Capacitación del personal.
- Filtros de correo electrónico.
- MFA (Multi-Factor Authentication / Autenticación Multifactor).

🔷 MITM

MITM (Man-In-The-Middle / Hombre en el Medio)

El atacante intercepta la comunicación entre dos partes sin que estas lo adviertan.

Impacto:

- Robo de datos sensibles.
- Manipulación de información en tránsito.

Controles relevantes:

- Encriptación SSL/TLS (Secure Sockets Layer / Transport Layer Security).
- Redes privadas virtuales VPN (Virtual Private Network / Red Privada Virtual).

🔷 Backdoor

Backdoor (Puerta Trasera)

Mecanismo oculto que permite acceso remoto no autorizado a un sistema.

Impacto:

- Control total del sistema.
- Persistencia del atacante.

Elementos críticos:

- Gestión de parches.
- Monitoreo de logs.
- Auditorías periódicas.

3️⃣ Ataques contra la Integridad de los Datos

🔷 SQL Injection

SQL (Structured Query Language / Lenguaje de Consulta Estructurado)

Consiste en insertar código malicioso en campos de entrada para manipular bases de datos.

Impacto:

- Modificación de registros.
- Acceso no autorizado.
- Eliminación de datos.

Medidas preventivas:

- Validación de datos de entrada.
- Uso de consultas parametrizadas.
- Auditorías de aplicaciones.

4️⃣ Ataques contra la Disponibilidad y Confidencialidad Simultáneamente

🔷 Ransomware

Software malicioso que cifra archivos y exige un rescate económico para liberarlos.

Impacto:

- Paralización total de operaciones.
- Pérdida de datos.
- Extorsión económica.

Elementos de TI estratégicos:

- Backups periódicos.
- Segmentación de red.
- Sistemas EDR (Endpoint Detection and Response / Detección y Respuesta en Endpoints).

Clasificación según el Pilar de Seguridad Afectado (Modelo CIA)

CIA (Confidentiality, Integrity, Availability / Confidencialidad, Integridad y Disponibilidad)

Ataque	Confidencialidad	Integridad	Disponibilidad
DDoS	❌	❌	✔️
Phishing	✔️	❌	❌
MITM	✔️	✔️	❌
Backdoor	✔️	✔️	✔️
SQL Injection	✔️	✔️	❌

Ataque	Confidencialidad	Integridad	Disponibilidad
Ransomware	✔	✔	✔

Enfoque para Administradores

Desde la mirada de la administración y los sistemas de información, estos ataques no deben analizarse únicamente como problemas técnicos, sino como riesgos estratégicos que impactan:

- Continuidad del negocio.
- Reputación institucional.
- Cumplimiento normativo.
- Confianza de clientes.
- Sostenibilidad financiera.

El diseño de arquitecturas seguras implica:

- Controles preventivos.
- Monitoreo continuo.
- Políticas claras.
- Capacitación permanente.
- Auditoría de sistemas.

La seguridad informática no es exclusivamente responsabilidad del área técnica; es una función estratégica de gobernanza organizacional.

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos),** los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.
La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.
Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.
Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.
Queda expresamente excluido cualquier uso con fines comerciales.