Universidad de Buenos Aires
Facultad de Ciencias Económicas

Dark y Deep Web

Material de Estudio

Traducción y Comentarios

SURFACE WEB, DEEP WEB y DARK WEB

La imagen representa la estructura de Internet mediante la metáfora de un iceberg. La parte visible sobre el agua simboliza la **Surface Web (Web Superficial)**, mientras que la parte sumergida representa la **Deep Web (Web Profunda)** y, en su zona más baja y restringida, la **Dark Web (Web Oscura)**.

---

1 Surface Web (Web Superficial)

Traducción de los ejemplos mostrados:

- Google
- Facebook
- Instagram
- YouTube

Definición

La **Surface Web (Web Superficial)** es la parte de Internet accesible públicamente y que puede ser indexada por motores de búsqueda como Google.

Características:

- Acceso abierto.
- Contenido indexado.
- Navegación estándar mediante navegadores comunes.
- Representa un porcentaje relativamente pequeño del total de información en Internet.

Desde la perspectiva de TI:

- Es el entorno más expuesto.
- Es donde operan los sitios corporativos.
- Es el principal punto de interacción con clientes.

Riesgos asociados:

- Ataques DDoS (Denial of Service / Denegación de Servicio).
- Phishing.
- Exposición de datos públicos mal gestionados.
- Ataques a reputación digital.

2️⃣ Deep Web (Web Profunda)

Traducción de los elementos mostrados:

- Medical Records → Registros médicos
- Legal Documents → Documentos legales
- Private Forums → Foros privados
- Research Papers → Artículos de investigación
- Non Indexed Content → Contenido no indexado

Definición

La **Deep Web (Web Profunda)** es la parte de Internet que no está indexada por motores de búsqueda y requiere autenticación o permisos específicos para acceder.

No es ilegal.

Simplemente no es pública.

Incluye:

- Bases de datos académicas.
- Sistemas bancarios.
- Intranets corporativas.

- Historias clínicas digitales.
- Sistemas ERP.
- Plataformas de gestión empresarial.

Desde la administración:

- Aquí se encuentra la información crítica.
- Representa el mayor volumen de datos organizacionales.
- Requiere controles estrictos de acceso.

Elementos clave de seguridad:

- IAM (Identity and Access Management / Gestión de Identidades y Accesos).
- MFA (Multi-Factor Authentication / Autenticación Multifactor).
- Cifrado de bases de datos.
- Segmentación de red.

La Deep Web es el verdadero núcleo operativo de las organizaciones digitales.

---

3 Dark Web (Web Oscura)

Traducción de los elementos mostrados:

- Private Communication Forums → Foros de comunicación privada
- TOR → The Onion Router (Red de anonimización por capas)
- Illegal Trade → Comercio ilegal
- Illegal Activities → Actividades ilegales

Definición

La **Dark Web (Web Oscura)** es una porción específica de la Deep Web que requiere software especializado para acceder, como:

- TOR (The Onion Router / Enrutador en Capas).

Características:

- Navegación anónima.
- Sitios no accesibles mediante navegadores tradicionales.
- Dominio .onion.

Importante aclaración:

La Dark Web no es sinónimo exclusivo de ilegalidad.

También es utilizada por:

- Periodistas.
- Activistas.
- Personas en regímenes autoritarios.
- Protección de privacidad.

Sin embargo, también alberga:

- Mercados ilícitos.
- Venta de datos robados.
- Comercio de malware.
- Fraude digital.

Comparación Estructural

Nivel	Accesibilidad	Legalidad	Uso Organizacional
Surface Web	Pública	Legal	Marketing, e-commerce
Deep Web	Privada	Legal	Sistemas internos, datos críticos
Dark Web	Anónima	Mixta	Riesgo reputacional y monitoreo

Enfoque para Estudiantes de Administración en TI

Desde la gestión de sistemas de información, la metáfora del iceberg permite comprender:

- La mayor parte de los activos críticos no es visible públicamente.
- La exposición en Surface Web debe gestionarse estratégicamente.
- La Deep Web requiere gobierno de datos y control interno.
- La Dark Web representa una dimensión de riesgo y monitoreo.

Implicancias Estratégicas

1️⃣ Protección de activos digitales.

2️⃣ Monitoreo de reputación y filtraciones en Dark Web.

3️⃣ Gestión de accesos en Deep Web.

4️⃣ Ciberinteligencia y análisis OSINT (Open Source Intelligence / Inteligencia de Fuentes Abiertas).

5️⃣ Gestión integral del riesgo digital.

Elementos Tecnológicos que Deben Considerarse

- Firewalls.
- Sistemas IDS/IPS (Intrusion Detection/Prevention System / Sistema de Detección y Prevención de Intrusiones).
- SIEM (Security Information and Event Management / Gestión de Eventos de Seguridad).
- Políticas de clasificación de información.
- Segmentación de red.
- Backup y DRP.

Conclusión Conceptual

La representación del iceberg evidencia que la parte visible de Internet es solo una fracción del ecosistema digital. La mayor parte de la información organizacional reside en la Deep Web, donde se gestionan datos sensibles y sistemas críticos. La Dark Web, aunque minoritaria en volumen, representa un foco relevante de riesgos estratégicos.

Para la administración moderna, comprender esta estructura es fundamental para diseñar políticas de seguridad, gestionar la exposición digital y proteger los activos informacionales que sostienen la continuidad y competitividad del negocio.

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.