# Facultad de Ciencias e Ingeniería

# Ingeniería Informática

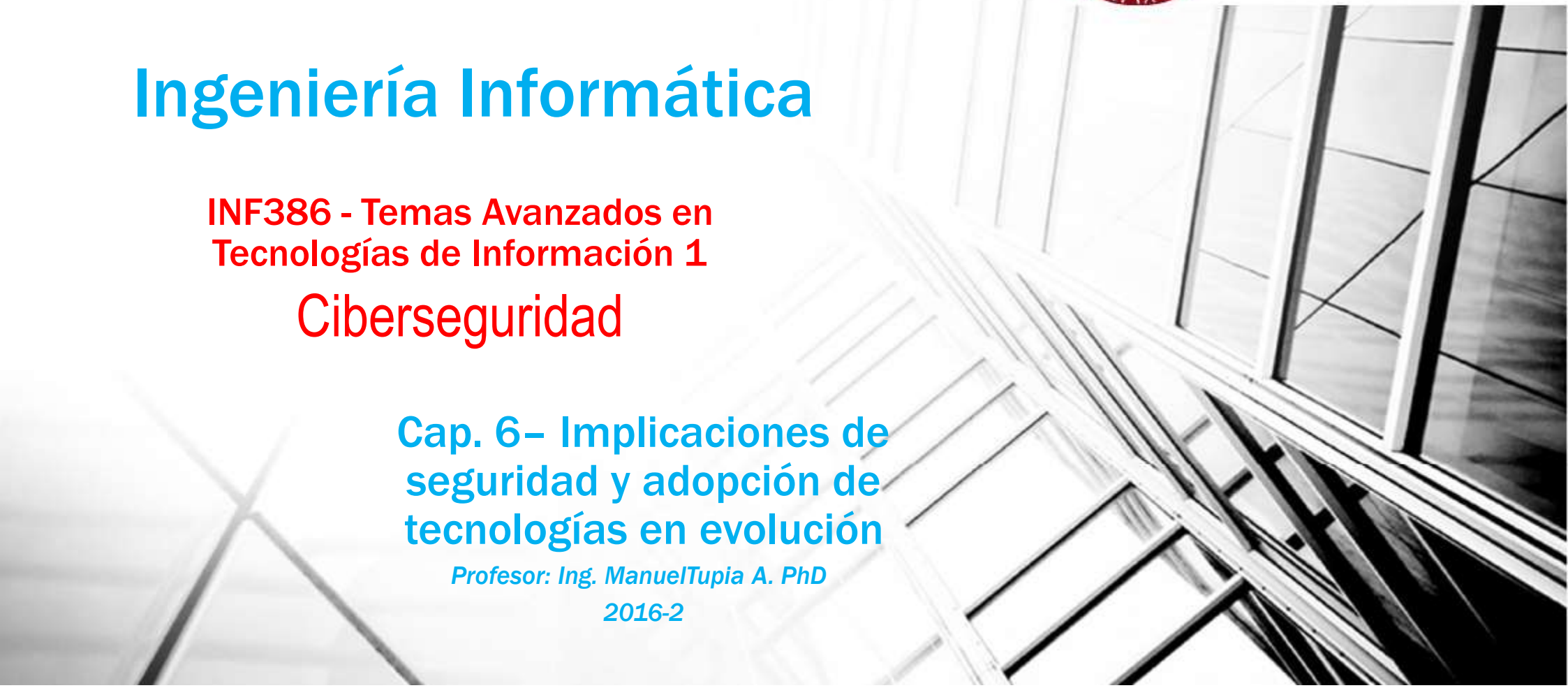
## INF386 - Temas Avanzados en Tecnologías de Información 1

## Ciberseguridad

## Cap. 6– Implicaciones de seguridad y adopción de tecnologías en evolución

*Profesor: Ing. ManuelTupia A. PhD*

*2016-2*



# Contenido


- Parte 1 – Escenario actual de las amenazas de ciberseguridad
- Parte 2 – Amenazas persistentes avanzadas
- Parte 3 – Tecnologías móviles: amenazas, vulnerabilidades y riesgos
- Parte 4 – Consumerización de las TIC
- Parte 5 – Cloud Computing
- Referencias bibliográficas

# Dominios de la Ciberseguridad

- ISACA ha establecido los siguientes dominios que tiene que conocer el profesional en Sistemas, Informática y ramas afines sobre ciberseguridad [ISACA, 2014]:
  - Conceptos de Seguridad Cibernética
  - Principios de Arquitectura de Seguridad
  - Seguridad de redes, sistemas, aplicaciones y datos
  - Respuesta a incidentes
  - Implicaciones de seguridad y adopción de Tecnologías en evolución

# Parte 1

## Escenario actual de las amenazas de ciberseguridad

# Escenario de amenaza

- El entorno de amenazas es una colección de amenazas.
- El panorama de las amenazas de ciberseguridad está constantemente cambiando y evolucionando a medida que se desarrollan nuevas tecnologías y se hacen más sofisticados los ciberataques y las herramientas para tales fines
- Las corporaciones están cada vez más dependientes de las tecnologías digitales que pueden ser susceptibles al riesgo de seguridad cibernética.
  - La computación en nube, las redes sociales y la informática móvil están cambiando la forma en que las organizacionesutilizan y comparten información.
  - Proporcionan mayores niveles de acceso y conectividad,lo que crea mayores aperturas para el cibercrimen.

# Escenario de amenaza

Business Continuity Institute

bsi.

# Escenario de amenaza

- Las tendencias recientes en el paisaje cibernético incluyen:
  - Los agentes de amenaza son más sofisticados en sus ataques y en el uso de herramientas.
  - Aplicación de patrones de ataque a dispositivos móviles. Esto es de especial interés para móviles y otros pequeños dispositivos digitales que están interconectados y a menudo tienen controles de seguridad deficientes.
  - La guerra cibernética.
  - La computación en nube resulta en grandes concentraciones de datos dentro de un pequeño número de instalaciones, convirtiéndose en atractivos y probables blancos para los atacantes.
  - Las redes sociales se han convertido en un canal primario de comunicación, recopilación de conocimientos, comercialización y difusión de información. Los atacantes pueden usar mal las redes sociales para obtener datos personales y promulgar información errónea.
  - Big data se refiere a grandes colecciones de datos estructurados y no estructurados y al uso de grandes infraestructuras, aplicaciones, servicios web y dispositivos. Su popularidad también hace que se vuelvan blanco de ataques.

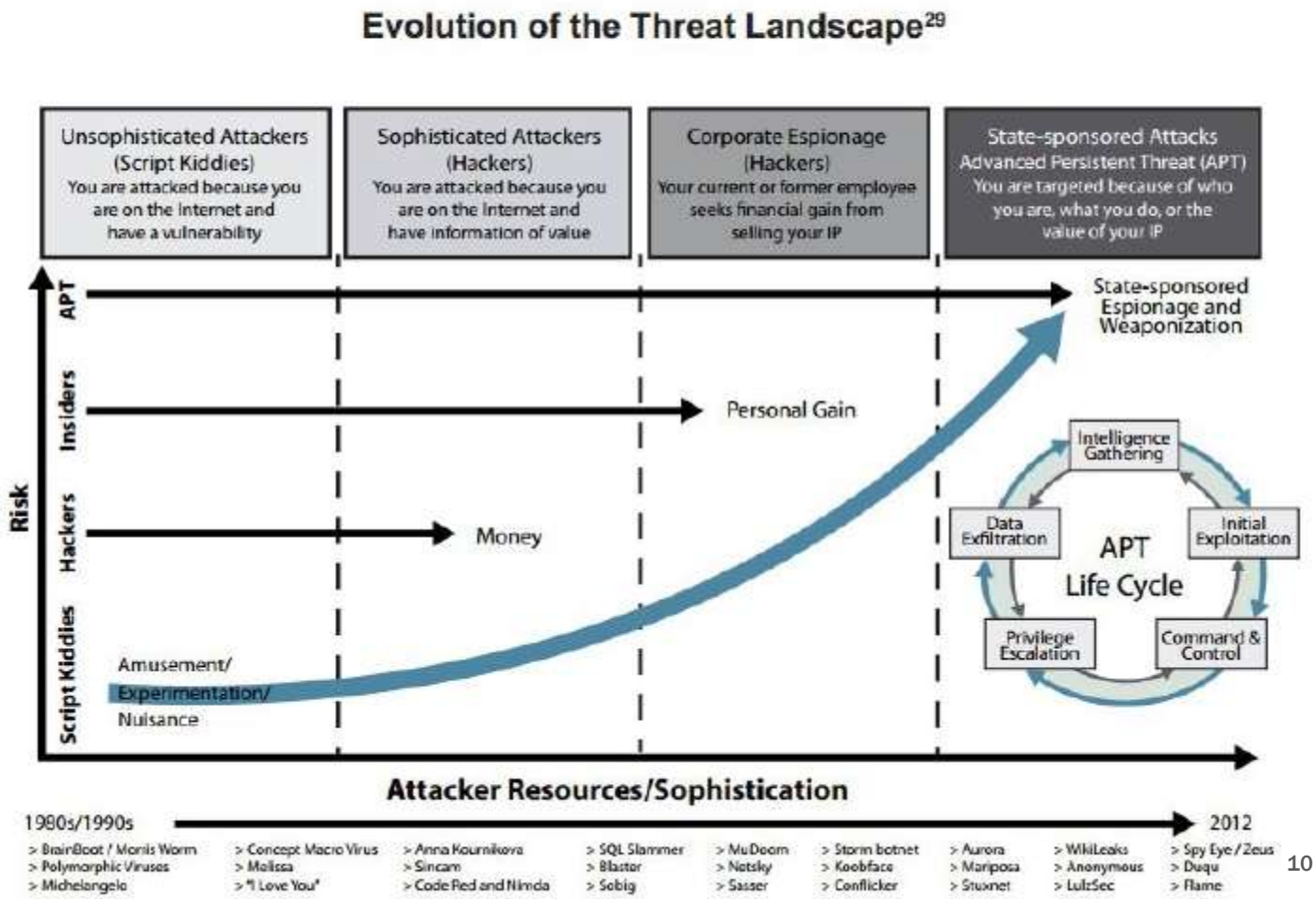
# Parte 2

## Amenazas persistentes avanzadas

# Amenazas persistentes avanzadas

- Las amenazas persistentes avanzadas (APT) son fenómenos relativamente nuevos para muchas organizaciones. Aunque los motivos detrás de ellos no son totalmente nuevos, el grado de planificación, los recursos empleados y las técnicas utilizadas en los ataques APT actualmente no tienen precedentes.
- Estas amenazas exigen un grado de vigilancia y un conjunto de contramedidas que están por encima del promedio utilizado por las empresas.

# Amenazas persistentes avanzadas



# Amenazas persistentes avanzadas

- Definición
  - No hay acuerdo.
  - Algunos expertos lo ven como la última evolución en las técnicas de ataque que se han ido desarrollando durante muchos años.
  - Otros afirman que el término es engañoso, señalando que muchos ataques clasificadoscomo APT no son especialmente inteligentes o novedosos.
  - Algunos lo definen en sus propios términos, por ejemplo, como un ataque que se maneja profesionalmente o que sigue un modus operandi particular, o uno lanzado por un servicio de inteligencia extranjero, o quizás uno que apunta incansablemente a (perjudicar a) una empresa específica.
  - De hecho, todas estas descripcionesson verdaderas.

# Amenazas persistentes avanzadas

- Características
  - Bien investigadas: los atacantes APT investigan a fondo sus objetivos, planifican el uso de los recursos y anticipan las contramedidas.
  - Sofisticadas:a menudo están diseñadospara explotar múltiples vulnerabilidadesen un solo ataque. Emplean un amplio marco de módulos de ataque diseñadospara ejecutar tareas automatizadasy orientarse a múltiples plataformas.
  - Sigilosas: a menudo pasan desapercibidosdurante meses y a veces años. No se anuncian y se “disfrazan” con diversas técnicas.
  - Persistentes:son proyectos a largo plazo, con enfoque en el reconocimiento.Si un ataque es bloqueado con éxito, los autores responden con nuevos ataques. Y, siempre están buscando mejores métodos o información para lanzar futuros ataques.

# Objetivos

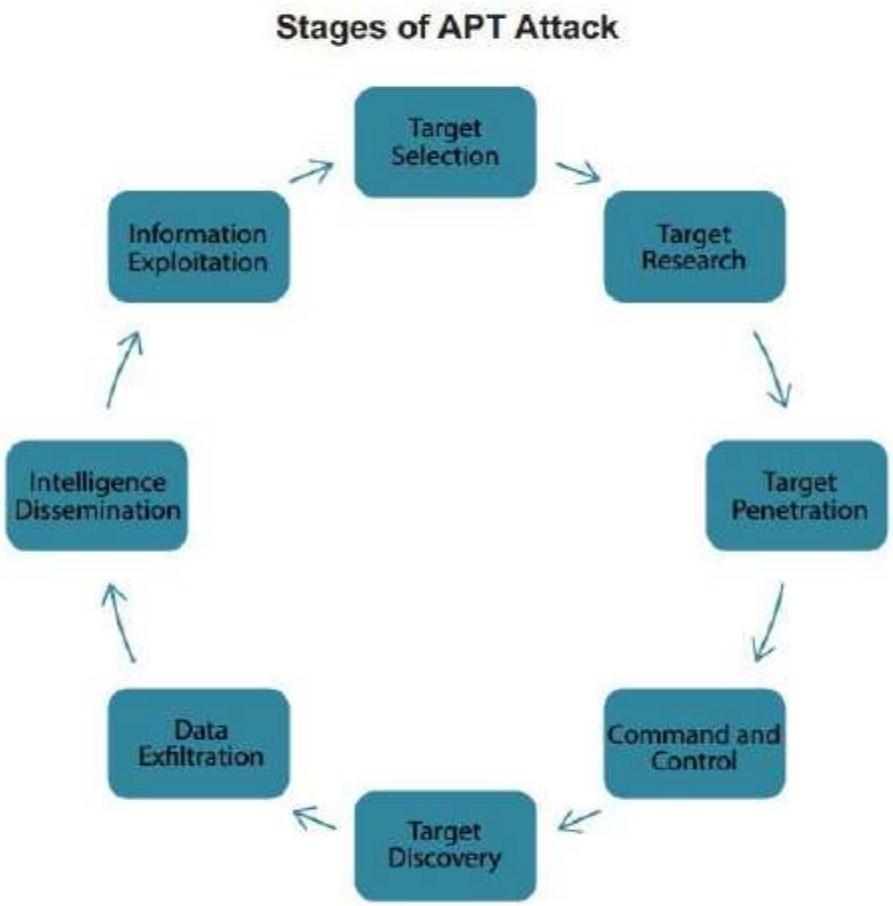
- Las APTs se dirigen a empresas de todos los tamaños, en todos los sectores de la industria y en todas las regiones geográficas que contienen activos de valor para los atacantes.
  - Ejemplo: el personal de todos los niveles de antigüedad, desde asistentes administrativos hasta directores ejecutivos, puede ser seleccionados como blanco de un ataque de phishing.
  - Las pequeñas empresas y hasta free-lancers podrían ser atacados porque son proveedores de servicios de una potencial víctima específica.
  - Los individuos pueden ser seleccionadossi son percibidos como un potencial escalón para ayudar a tener accesoal objetivo final.
- Ninguna industria con secretos valiosos u otras fuentes de ventajas comerciales que puedan ser copiadas o socavadas por el espionaje está a salvo de un ataque de APT.
- Ninguna empresa que controle transferencias de dinero, procese datos de tarjetas de crédito o almacene datos personales identificables en individuos puede dejar de ser protegida de ataques criminales.
- Del mismo modo, ninguna industria que suministre o apoye la infraestructura nacional crítica es inmune a una intrusión de los ciberguerreros.

# Objetivos

| Threat | What They Seek | Business Impact |
|---|---|---|
| Intelligence agencies | Political, defense or commercial trade secrets | Loss of trade secrets or commercial, competitive advantage |
| Criminal groups | Money transfers, extortion opportunities, personal identity information or any secrets for potential onward sale | Financial loss, large-scale customer data breach or loss of trade secrets |
| Terrorist groups | Production of widespread terror through death, destruction and disruption | Loss of production and services, stock market irregularities, and potential risk to human life |

| Threat | What They Seek | Business Impact |
|---|---|---|
| Activist groups | Confidential information or disruption of services | Major data breach or loss of service |
| Armed forces | Intelligence or positioning to support future attacks on critical national infrastructure | Serious damage to facilities in the event of a military conflict |

# Fases de un APT



# Parte 3

## Tecnologías móviles: amenazas, vulnerabilidades y riesgos

# Tecnologías móviles: amenazas, vulnerabilidades y riesgos

| Mobile Technology Vulnerabilities, Threats and Risk[30] | | |
|---|---|---|
| **Vulnerability** | **Threat** | **Risk** |
| Information travels across wireless networks that are often less secure than wired networks. | Malicious outsiders can do harm to the enterprise. | Information interception resulting in a breach of sensitive data, damage to enterprise reputation, compromised adherence to regulation or legal action |
| Mobility provides the users with the opportunity to leave enterprise boundaries, thereby eliminating many security controls. | Mobile devices cross boundaries and network perimeters, carrying malware, and can bring this malware into the enterprise network. | Malware propagation, which can result in data leakage, data corruption and unavailability of necessary data<br>Physical theft |
| Bluetooth (BT) technology makes it very convenient for many users to have hands-free conversations; however, it is often left on and is then discoverable. | Hackers can discover the device and then launch an attack. | Device corruption, lost data, call interception, possible exposure of sensitive information |
| Unencrypted information is stored on the device. | In the event that a malicious outsider intercepts data in transit or steals a device, or if the employee loses the device, the data are readable and usable. | Exposure of sensitive data, resulting in damage to the enterprise, customers or employees |
| Lost data may affect employee productivity. | Mobile devices may be lost or stolen due to their portability. Data on these devices are not always backed up. | Workers dependent on mobile devices unable to work in the event of broken, lost or stolen devices, and data that are not backed up |
| The device has no authentication requirements applied. | If the device is lost or stolen, outsiders can access the device and all its data. | Data exposure, resulting in damage to the enterprise and liability and regulation issues |
| The enterprise is not managing the device. | If no mobile device strategy exists, employees may choose to bring in their own, unsecured devices. While these devices may not connect to the virtual private network (VPN), they may interact with emails or store sensitive documents. | Data leakage, malware propagation, unknown data loss in the event of device loss or theft |

# Riesgos físicos

- Se pierden fácilmente (o son robados), particularmente en áreas públicas.
  - Esto aumenta el riesgo físico general, dado que los teléfonos inteligentes avanzados a menudo son vistos como objetivos interesantes para los delincuentescomunes.
  - A medida que los usuarios confían cada vez más en sus dispositivos móviles, la pérdida o robo es más probable que cree condicionesde perturbación y puede dejar a los empleados incapaces de trabajar por períodos prolongados de tiempo.
  - Las consecuenciasde seguridad de la pérdida de dispositivos son más graves.
    - Por ejemplo, los datos no protegidos y transitorios, como listas de llamadas, textos o elementos del calendario, pueden verse comprometidos, lo que permite a los atacantes recolectar grandes cantidades de datos.
    - Con intención criminal, los autores pueden ser capaces de recuperar los datos borrados y un historial del uso del dispositivo móvil.
    - Posibilidad de robo de identidad

# Riesgos físicos

- Desde una perspectiva de gestión de la seguridad, se han realizado varios intentos para prevenir, o al menos mitigar, la amenaza de pérdida o robo de dispositivos:
  - Seguimiento y localización de dispositivos basados en celdas (Cell-based tracking and locating the device)
  - Funciones de apagado / borrado remoto
  - Funciones de bloqueo remoto de la tarjeta SIM
- Si bien estas instalaciones proporcionan un grado de seguridad, todavía dejan una ventana de exposición a los atacantes que exploran el dispositivo, posiblemente utilizando herramientas analíticas que burlarán las características estándar del sistema operativo.
  - Restricciones de protección por las limitaciones que plantean los sistemas operativos.

# Riesgos organizacionales

- Como con muchas otras tecnologías, los dispositivos móviles han penetrado rápidamente las empresas en todos los niveles.
  - (BYOD)
- En términos de datos, información y conocimiento que existen en la empresa, muchos usuarios tienen acceso a dicha información (privilegiada) a través de sus dispositivos móviles.
- Mientras que los entornos corporativos de PC han sido objeto de medidas de endurecimiento y protección durante muchos años, los dispositivos móviles y sus comparativamente débiles mecanismos de seguridad son más difíciles de manejar y controlar.
  - Diversidad de dispositivos

# Riesgos técnicos

| Activity Monitoring and Data Retrieval Risk[31] | |
|---|---|
| **Target** | **Risk** |
| Messaging | Generic attacks on SMS text, MMS-enriched transmission of text and contents |
| | Retrieval of online and offline email contents |
| | Insertion of service commands by SMS cell broadcast texts |
| | Arbitrary code execution via SMS/MMS |
| | Redirect or phishing attacks by HTML-enabled SMS text or email |
| Audio | Covert call initiation, call recording |
| | Open microphone recording |
| Pictures/Video | Retrieval of still pictures and videos, for instance, by piggybacking the usual "share" functionality in most mobile apps |
| | Covert picture or video taking and sharing, including traceless wiping of such material |

| Activity Monitoring and Data Retrieval Risk[31] | |
|---|---|
| **Target** | **Risk** |
| Geolocation | Monitoring and retrieval of GPS positioning data, including date and time stamps |
| Static data | Contact list, calendar, tasks, notes retrieval |
| History | Monitoring and retrieval of all history files in the device or on SIM card (calls, SMS, browsing, input, stored passwords, etc.) |
| Storage | Generic attacks on device storage (hard disk or solid state disk [SSD]) and data replicated there |

# Riesgos técnicos

| Sensitive Data Leakage Risk[33] | |
|---|---|
| **Type of Information** | **Risk** |
| Identity | International Mobile Equipment Identity (IMEI), manufacturer device ID, customized user information |
| | Hardware/firmware and software release stats, also disclosing known weaknesses or potential zero-day exploits |
| Credentials | User names and passwords, keystrokes |
| | Authorization tokens, certificates (S/MIME, PGP, etc.) |
| Location | GPS coordinates, movement tracking, location/behavioral inference |
| Files | All files stored at operating system/file system level |

# Parte 4

## Consumerización de las TIC

# Introducción

- La consumerización es la tendencia creciente según la cual los usuarios corporativos terminan por decidir qué dispositivos, aplicaciones y servicios se usan en el empleo.
- Las nuevas ~~tecnologías de la información~~ surgen primero en el mercado del ~~consumidor~~ y luego se propagan hacia las organizaciones comerciales y gubernamentales.
- El establecimiento de los mercados de los consumidores como los impulsores primarios de la innovación en la tecnología de la información se vislumbra como un cambio grande en el ámbito de la tecnología informática, ya que las primeras décadas del desarrollo y el uso de las computadoras estuvieron dominadas por las grandes empresas y organizaciones de gobierno

# Consumerización

- Los dispositivos móviles han tenido un profundo impacto en la forma en que se conduce el negocio y en los patrones de comportamiento en la sociedad.
- Han aumentado considerablemente la productividad y flexibilidad en el lugar de trabajo, en la medida en que las personas están ahora en condiciones de trabajar desde cualquier lugar en cualquier momento dado.
- Del mismo modo, la potencia de cálculo de los dispositivos inteligentes les ha permitido reemplazar PCs de escritorio y portátiles para muchas aplicaciones empresariales.
- Tanto los fabricantes como los proveedores de servicios han creado tanto nuevos dispositivos como nuevos modelos de negocio, como pagos móviles o descargas de suscripciones, utilizando un modelo de pago por uso.
  - Cloud Computing

# Consumerización

- El impacto del uso de dispositivos móviles se divide en dos grandes categorías:
  - El propio hardware se ha desarrolladohasta un nivel en el que la potencia de cálculo y el almacenamientoson casi equivalentes al hardware de PC.
  - Los nuevos servicios móviles han creado nuevos modelos de negocio que están cambiando las estructurasorganizacionalesy la sociedad en su conjunto.
- La consumerización no se limita a los dispositivos. Las nuevas aplicaciones y servicios de libre acceso brindan mejores experiencias de usuario para actividades como la toma de notas, la videoconferencia, el correo electrónico y el almacenamiento en la nube que sus respectivas contrapartes corporativas. En lugar de contar con dispositivos y software de la empresa, los empleados están utilizando sus propias soluciones que mejor encajan con su estilo de vida, las necesidades de los usuarios y las preferencias.

# BYOD

- La movilidad general y la accesibilidad independiente de la ubicación han mejorado las prácticas empresariales y han permitido a las empresas concentrarse en las actividades básicas, reduciendo al mismo tiempo la cantidad de espacio de oficinas utilizada.
- Para los empleados, los dispositivos móviles han aportado una mayor flexibilidad, por ejemplo, en llevar a su propio dispositivo (BYOD)
- La idea de utilizar dispositivos móviles de propiedad privada se ha convertido rápidamente en un concepto, y muchas empresas se enfrentan ahora a un nuevo obstáculo: cuando la adquisición centralizada y el aprovisionamiento de dispositivos móviles son lentos o engorrosos, muchos usuarios han optado por instalar sus propios dispositivos.
- **Todo el escenario anterior conlleva a la aparición de riesgos de ciberataque que las empresas no están preparadas a sobrellevar, sobre todo cuando los equipos no les pertencen.**

# BYOD

Pros and Cons of BYOD

| Pros | Cons |
| --- | --- |
| • Shifts costs to user | • IT loss of control |
| • Worker satisfaction | • Known or unknown security risk |
| • More frequent hardware upgrades | • Acceptable Use Policy is more difficult to implement |
| • Cutting-edge technology with the latest features and capabilities | • Unclear compliance and ownership of data |

# Parte 5

## Cloud Computing

# Cloud computing

- Según NIST y Cloud Security Alliance (CSA), el cloud computing se define como un "modelo para permitir un acceso conveniente a la demanda a un conjunto compartido de recursos computacionales configurables (por ejemplo, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provisionados y liberados con un mínimo esfuerzo de gestión o interacción con el proveedor de servicios“ [CSA, 2013].
  - Los tipos de servicio que se ofrecen en la nube incluyen:
    - Software como Servicio (SaaS)
    - Plataforma como Servicio (PaaS)
    - Infraestructura como Servicio (IaaS)
- La virtualización y las arquitecturas orientadas a servicios (SOA) actúan como elementos clave detrás de las escenas. A pesar de ser atractiva, la computación en la nube no está exenta de su propio conjunto de riesgos, en primer lugar y sobre todo de la seguridad de los datos que se confían en el cuidado de los proveedores de la nube.
- Este modelo de prestación de servicios de TI también está sujeto de ataques por parte de ciberdelincuentes

# Amenazas de Cloud Computing

- Brecha de datos
- Pérdida de datos
- Suplantación de identidades de usuario o secuestros de cuentas de usuario
- APIs inseguras
- DoS
- Personal malicioso dentro del staff del proveedor Cloud
- Abuso o mal uso de los servicios Cloud
- Insuficiente “due diligence”: pobreza en las auditorías

# Riesgos de Cloud Computing

**Risk of Cloud Computing**

The challenge for cloud computing is to protect data within public and private clouds as well as ensure governance, risk management and compliance are addressed across the full, integrated environment. NIST outlines the following top security risks for cloud infrastructure:

- **Loss of governance**—The client usually relinquishes some level of control to the cloud provider, which may affect security, especially if the SLAs leave a gap in security defenses.
- **Lock-in**—It can be difficult for a client to migrate from one provider to another, which creates a dependency on a particular cloud provider for service provision.
- **Isolation failure**—One characteristic of cloud computing is shared resources. Although not commonplace, the failure of mechanisms that separate storage, memory, routing and reputation between different tenants can create risk.
- **Compliance**—Migrating to the cloud may create a risk in the organization achieving certification if the cloud provider cannot provide compliance evidence.
- **Management interface compromise**—The customer management interface can pose an increased risk because it is accessed through the Internet and mediates access to larger sets of resources.
- **Data protection**—It may be difficult for clients to check the data handling procedures of the cloud provider.
- **Insecure or incomplete data deletion**—Because of the multiple tenancies and the reuse of hardware resources, there is a greater risk that data are not deleted completely, adequately, or in a timely manner.
- **Malicious insider**—Cloud architects have extremely high-risk roles. A malicious insider could cause a great degree of damage.

# Referencias


- [CSA, 2013] Cloud Security Alliance (CSA), *The Notorious Nine: Cloud Computing Top Threats in 2013*, USA (2013)
- [ISACA, 2014] ISACA. *Cybersecurity Fundamentals Study Guide.* ISACA Publishing, USA (2014)
- [ISO, 2013] International Organization for Standardization. *ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security management*. ISO, 2013.
- [McKemmish , 2003] McKemmish D. R. *Computer and Intrusion Forensics*, Artech House, USA, 2003
- [Schultz, Brown, and Longstaff, 1990]Schultz, E.E., Brown, D.S., and Longstaff, T.A.; *Responding to Computer Security Incidents: Guidelines for Incident Handling,* Lawrence Livermore National Lab., USA, 1990