6669 Criptografía y Seguridad Informática

Introducción

Código: **66.69 / 86.36**

Materia: **Criptografía y Seguridad Informática**
Departamento: **Electrónica**
Créditos: **6**

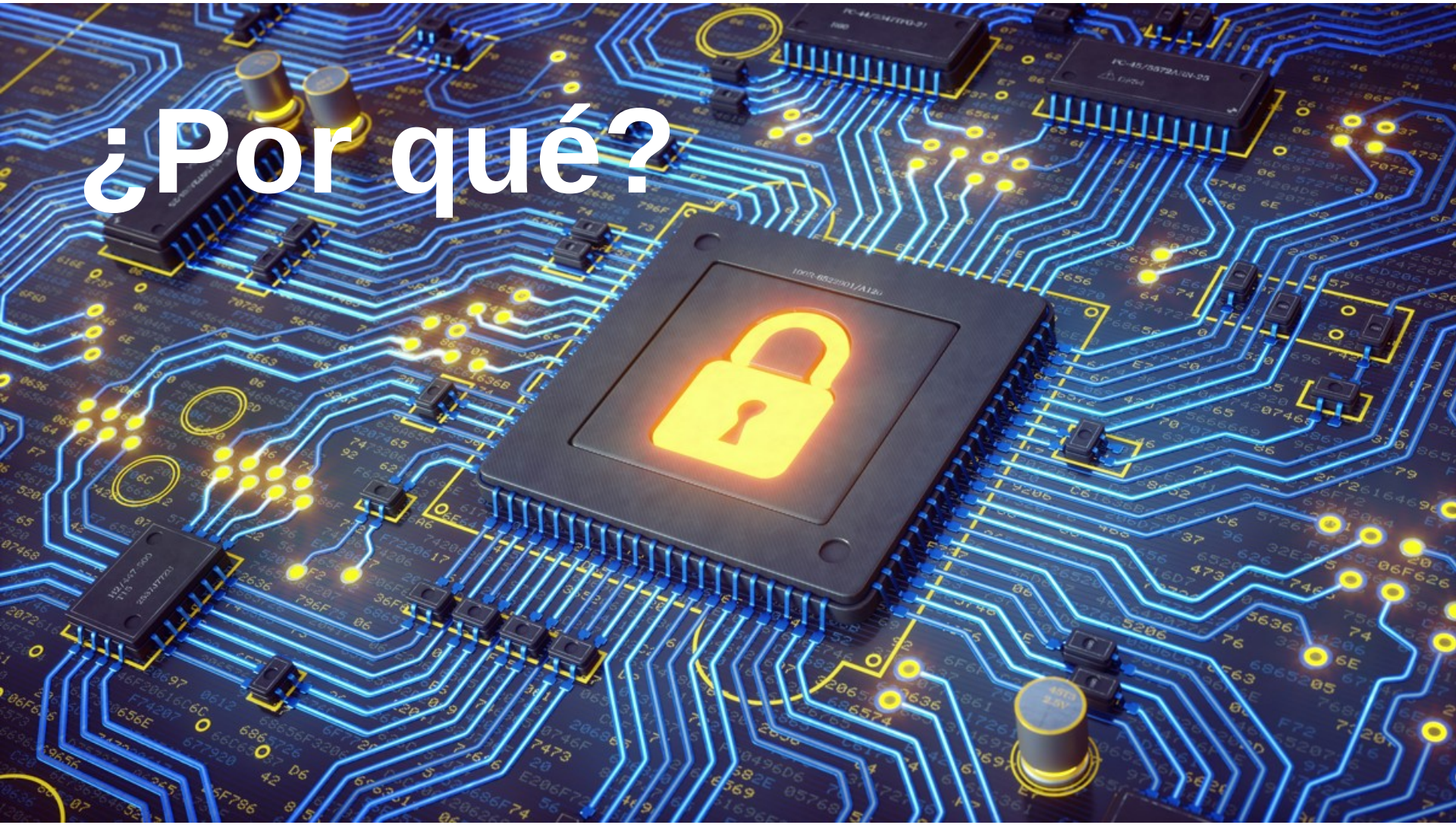
Ingeniería Electrónica
86.05 Señales y Sistemas
86.07 Laboratorio de Microcomputadoras

Ingeniería Informática
75.43 Introducción a los Sistemas Distribuidos

Lic. Análisis de Sistemas
95.60 Redes y Aplicaciones Distribuida

Docentes:
Ing. Hugo Pagola
Lic. Javier Vallejos JTP
Pablo Peiretti

Horarios:
Lunes y Viernes 19.30 a 22.30


¿Por qué?

Crypto AG

Con la inteligencia alemana

El truco que usó la CIA para espiar a la Argentina y otros 120 países aliados y enemigos durante más de 50 años

Lo hizo a través de una compañía suiza que vendía a gobiernos de todo el mundo máquinas para descifrar mensajes encriptados. Entre otros acontecimientos, alimentaron de datos a Gran Bretaña en la guerra de Malvinas.

Crypto AG

https://www.swissinfo.ch/eng/politics/crypto-spying-affair_how-manipulated-swiss-tech-shaped-world-pc

fo.ch | #20yearsSWI

From left to right: Sadat, Carter, Begin sign the Camp David Peace Accords between Egypt and Israel in March 1979.

(Keystone / Str)

Camp David, Iran, Argentina, Panama: These are just a few examples of how the US steered world politics with decoded messages "encrypted" with Swiss machines.

A 280-page secret service dossier by the CIA and the German Federal Intelligence Service (BND) proves that for decades, there has been espionage via manipulated encryption devices from the Swiss company Crypto AG. More than 100 countries bought the encryption devices from the Zug-based company, which did business under the guise of Swiss neutrality, but in reality, belonged to the CIA and the BND.

With the help of the intercepted, supposedly encrypted communications of several countries, world politics were influenced. Below are four examples.

Camp David

September 1978. A good ten years after the Six-Day War, in which Egypt, Syria and Jordan suffered a heavy defeat and land losses against Israel, US President Jimmy Carter launched a Middle East initiative. It was supposed to finally bring peace between Israel and Egypt, and there was great mistrust among

https://www.swissinfo.ch/eng/politics/crypto-spying-affair_how-manipulated-swiss-tech-shaped-world-politics/45554828

Ciberataque a Ucrania

https://www.infosecurity-magazine.com/opinions/blackenergy-malware-infrastructure/

7 FEB 2018 OPINION

BlackEnergy Malware: How Hackers May Tackle our Infrastructure

Adam Vincent CEO of ThreatConnect
Follow @threatconnect

On December 23 2015, 230,000 people in Ukraine were left in the dark for six hours after hackers compromised several power distribution centres which provide electricity to residents in Ukraine. The attackers used spear phishing emails and variants of the BlackEnergy 3 malware to gain a foothold into the IT networks of the electricity companies and knock real-world systems offline.

This incident was the first recorded successful cyber-attack on an electric grid - and if a power outage at the beginning of winter doesn't sound too bad, just consider the impact if such a breach were to affect the country's hospitals.

Energy hacks: 2018 model

Attackers are becoming smarter and more apt, illustrating a degree of learning which is concerning to the security community. In 2018, we'll likely see threat actors increase their focus on critical infrastructure.

It's often said that the great battles of the 21st Century will take place online, and with the example of the Ukrainian attack it's not hard to see why. Imagine if a hostile actor hacked into the rail signaling network and crashed speeding trains into one another; or if the power in Parliament was cut for days. As we connect more of our critical infrastructure to the internet

Related to This Story

Red October cyber-espionage campaign u
sophisticated infiltration techniques

Don't Get Complacent About Ransomwar

Cisco: Destructive VPNFilter Malware Ha
500K Devices

Five Security "Gotchas" for MSPs

Punycode: Undetectable, but not Unbeat

What's Hot on Infosecurity Magaz

Read | Shared | Watched | Editor

Ciberataque a Ucrania

- Diciembre de 2015, Ucrania experimentó un asalto en su red eléctrica. El ataque causó cortes de electricidad generalizados.
- Los atacantes se infiltraron en tres compañías energéticas y cerraron temporalmente la generación de energía en tres regiones de Ucrania.
- Los atacantes utilizaron el programa malicioso BlackEnergy 3 para cerrar las tres subestaciones. Se distribuyó mediante correos electrónicos de *phishing* personalizado.

Enron: 2 de diciembre de 2001

- Uno de los mayores **escándalos** de la historia económica.
  - La empresa energética Enron se declaraba en quiebra.
  - Primer distribuidor energético a nivel global, facturaba **100.000 millones de dólares anuales**.
- **Ingeniería contable:**
  - Pasivos que se convirtieron en activos
  - Préstamos que se computaban como ingresos
  - Deuda maquillada, beneficios inflados

EL PAÍS NEGOCIO

Enron cae en su propia 'trampa'

El gigante energético sucumbe a las originales normas contables que él mismo impulsó

RICARDO MARTÍNEZ DE RITUERTO

10 DIC 2001

Enron, el gigante energético norteamericano, se ha estrellado. Ha protagonizado la mayor suspensión de pagos de la historia y ha provocado que el Congreso de Estados Unidos comience a analizar en enero los cambios necesarios para evitar otros fiasco semejante y si hay que retocar la apresurada liberalización del mercado energético, en especial el de la electricidad.

Kanneth Lay, presidente de Enron AP

La compañía presenta unos activos de 49.800

'Es muy preocupante que una compañía pueda hundirse tanto y tan deprisa'. Las palabras del congresista Billy Tauzin,

HOME SEARCH The New York Times

Who Killed Andersen? It Was Suicide

By FLOYD NORRIS JUNE 3, 2005

WHO, or what, killed Arthur Andersen? Was it David B. Duncan, the auditor with the shredding machine, or was it a group of overzealous prosecutors?

The answer is that it was neither. Andersen was killed by its management, which penalized good auditors while rewarding those who made companies happy.

This week, as the Supreme Court reversed Andersen's criminal conviction for the shredding of Enron documents, the opinion by Chief Justice William H. Rehnquist stated, in passing, "It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy."

But the history of that document retention policy was at the heart of Andersen's demise. It was written by a partner named Robert G. Kutsenda while he was under investigation for his role in accounting fraud at Waste Management. He and his bosses knew he was in trouble because the

Arthur Andersen

ARTHURANDERSEN

Empresa

Arthur Andersen LLP fue una empresa fundada en 1913 que llegó a convertirse en una de las cinco mayores compañías auditoras del mundo, hasta su práctica desaparición en 2002 a raíz del escándalo Enron. Su sede se encontraba en Chicago. Wikipedia

Fundación: 1913

Oficinas centrales: St. Charles, Illinois, Estados Unidos

Fundadores: Arthur E. Andersen, Clarence DeLany

EL PAÍS

ECONOMÍA

El fraude contable de WorldCom es casi el doble de lo estimado

Los auditores descubren otros 3.416 millones en partidas falsas

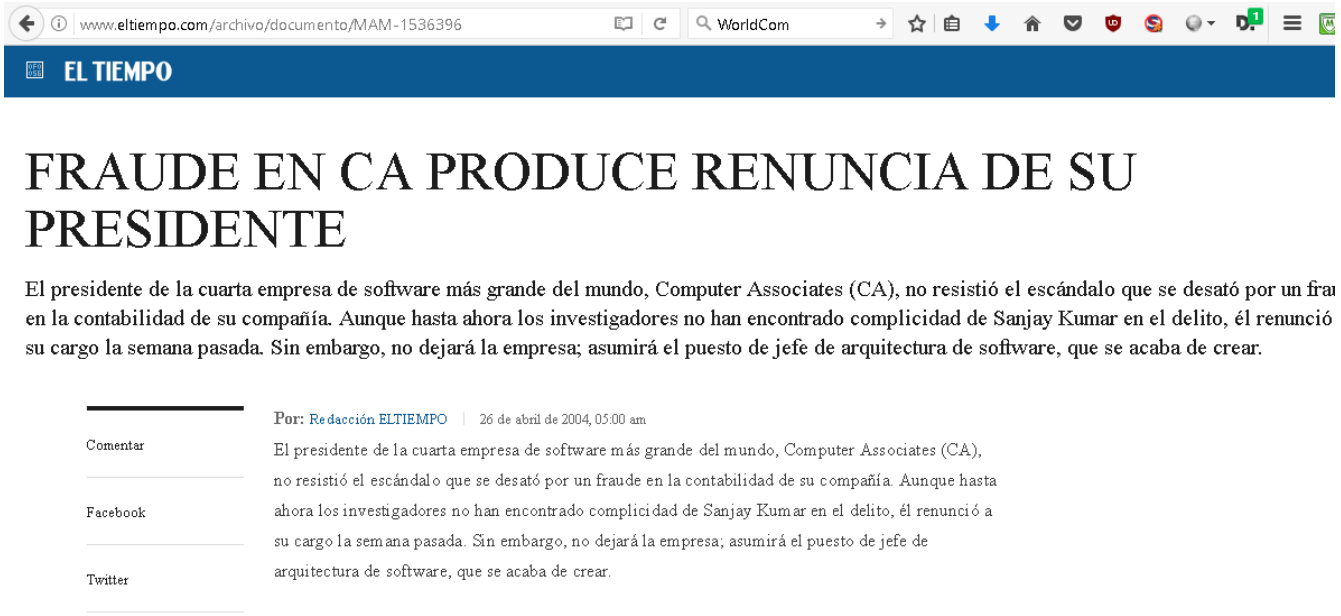
AGENCIAS

Nueva York - 9 AGO 2002

Los auditores han detectado en la compañía de telefonía WorldCom nuevos *errores* contables, por valor de 3.300 millones de dólares (unos 3.416 millones de euros), con lo que la cifra mal registrada en libros alcanza 7.180 millones de dólares, según informó ayer la actual administración de la empresa. El *caso WorldCom* forzó en julio pasado la suspensión de pagos de la firma, la mayor de la historia de EE UU.

MÁS INFORMACIÓN

Tras una segunda revisión de su contabilidad, WorldCom reveló irregularidades en el registro de cuentas por otros 3.300



www.eltiempo.com/archivo/documento/MAM-1536396

WorldCom

EL TIEMPO

FRAUDE EN CA PRODUCE RENUNCIA DE SU PRESIDENTE

El presidente de la cuarta empresa de software más grande del mundo, Computer Associates (CA), no resistió el escándalo que se desató por un frau en la contabilidad de su compañía. Aunque hasta ahora los investigadores no han encontrado complicidad de Sanjay Kumar en el delito, él renunció su cargo la semana pasada. Sin embargo, no dejará la empresa; asumirá el puesto de jefe de arquitectura de software, que se acaba de crear.

Comentar

Facebook

Twitter

Por: Redacción ELTIEMPO | 26 de abril de 2004, 05:00 am

El presidente de la cuarta empresa de software más grande del mundo, Computer Associates (CA), no resistió el escándalo que se desató por un fraude en la contabilidad de su compañía. Aunque hasta ahora los investigadores no han encontrado complicidad de Sanjay Kumar en el delito, él renunció a su cargo la semana pasada. Sin embargo, no dejará la empresa; asumirá el puesto de jefe de arquitectura de software, que se acaba de crear.

- Según la SEC, en el año 2000 la empresa reportó antes de tiempo más de 1.400 millones de dólares en ingresos de 116 contratos.
- Estos negocios se firmaron cuando el trimestre contable en el que se registraron ya se había cerrado, y sumaban un tercio de los ingresos de la compañía en ese período.

El factor común es la alteración de los datos que están en los sistemas de las organizaciones con el fin de mostrar una situación financiera diferente a la real.

SOX

El acta (Act) Sarbanes-Oxley (SOA) ha vuelto a definir las responsabilidades de la dirección ejecutiva y consejos de administración en las organizaciones, las expectativas de los inversores, reguladores e interesados del negocio externos.

- Parar el Fraude Fiscal
- Las organizaciones son legalmente responsables de decir la verdad a los inversores.
- Aumentó la responsabilidad de las empresas auditoras de permanecer independientes.

https://www.thebalance.com/sarbanes-oxley-act-of-2002-3306254

Auditoria SOX

- Por fallas del control interno se filtraba información sensible antes de que fuera pública. => se vendía la información y los amigos podían comprar o vender antes de que sea pública.
- El Acta SOX apunta a tener mayor control interno en las empresas. Tanto contable, de operaciones y de IT

Normativas

- **Comunicación “A” 4609 del BCRA para entidades Financieras**

Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información.

- **ISO/IEC 27001**

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI)

-

Basilea II

Estandar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

Ley Sarbanes Oxley (SOX)

Impulsada por el gobierno norteamericano como respuesta a los mega fraudes corporativos que impulsaron Enron, Tyco International, WorldCom. Es un conjunto de medidas tendientes a asegurar la efectividad de los controles internos sobre reportes financieros.

Protección de Datos Personales
Ley 25.326

Dato personal

- Toda información relativa a una persona física o jurídica

Requisitos para el tratamiento de datos personales

- Consentimiento libre, expreso e informado del Titular de los datos
- Existen algunas excepciones al consentimiento, tales como DNI, Nombre, ocupación, domicilio, etc.

Derechos del titular

- Controlar el tratamiento de sus datos personales
- Acceder a sus datos personales contenidos en archivos de terceros
- Solicitar supresión, actualización o corrección de sus datos personales

Ley N° 11.723/25.036
Propiedad Intelectual

➔¿Qué protege?

- Los derechos de autor de los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

➔Consecuencias

- La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

fuente ARCERT

Ley N° 25.506 – Firma Digital

Se reconoce la eficacia jurídica al empleo de la Firma Digital.

➔ Documento Digital

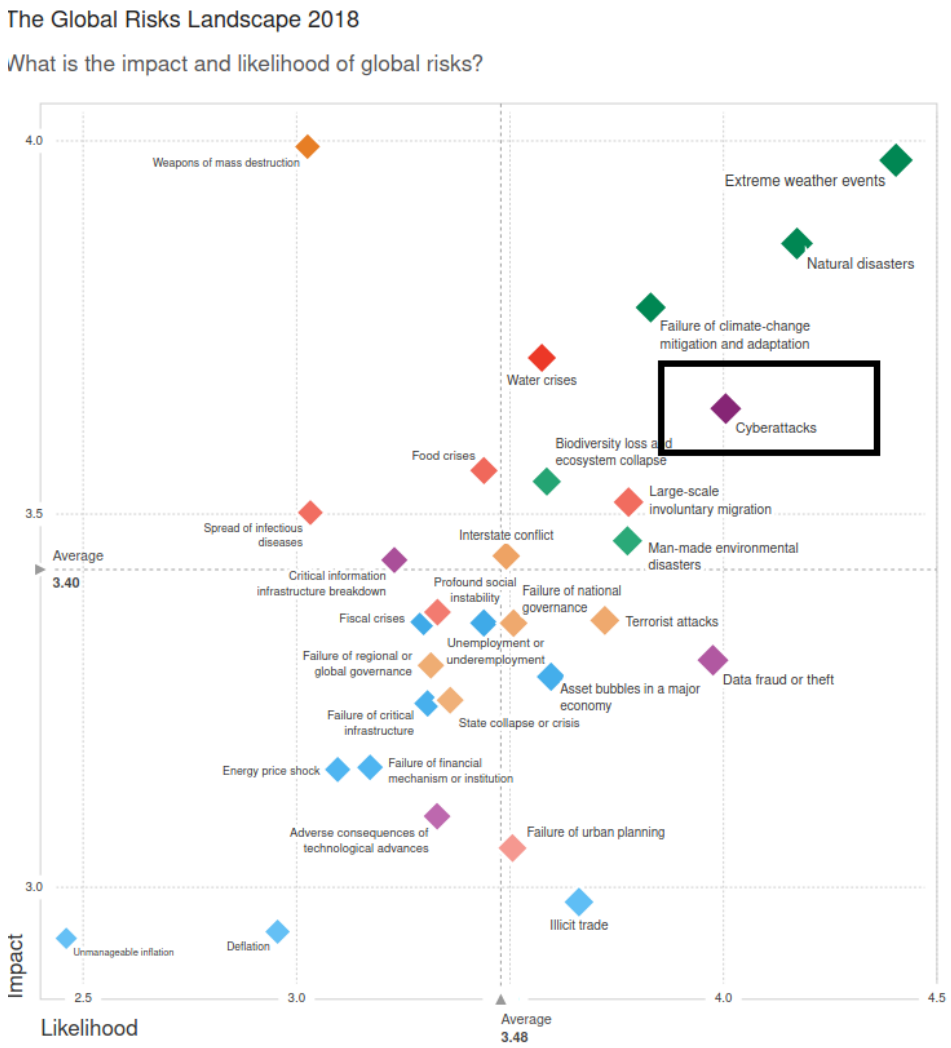
… Representación digital de actos o hechos con independencia del soporte utilizado para su fijación, almacenamiento o archivo …

➔ Firma Digital

… Resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante

fuente ARCERT

WEF Panorama Global de Riesgos



http://reports.weforum.org/global-risks-2018/global-risks-landscape-2018/#landscape

FIGURE E

Global risks ranked by severity

"Please estimate the likely impact (severity) of the following risks over a 2-year and 10-year period"

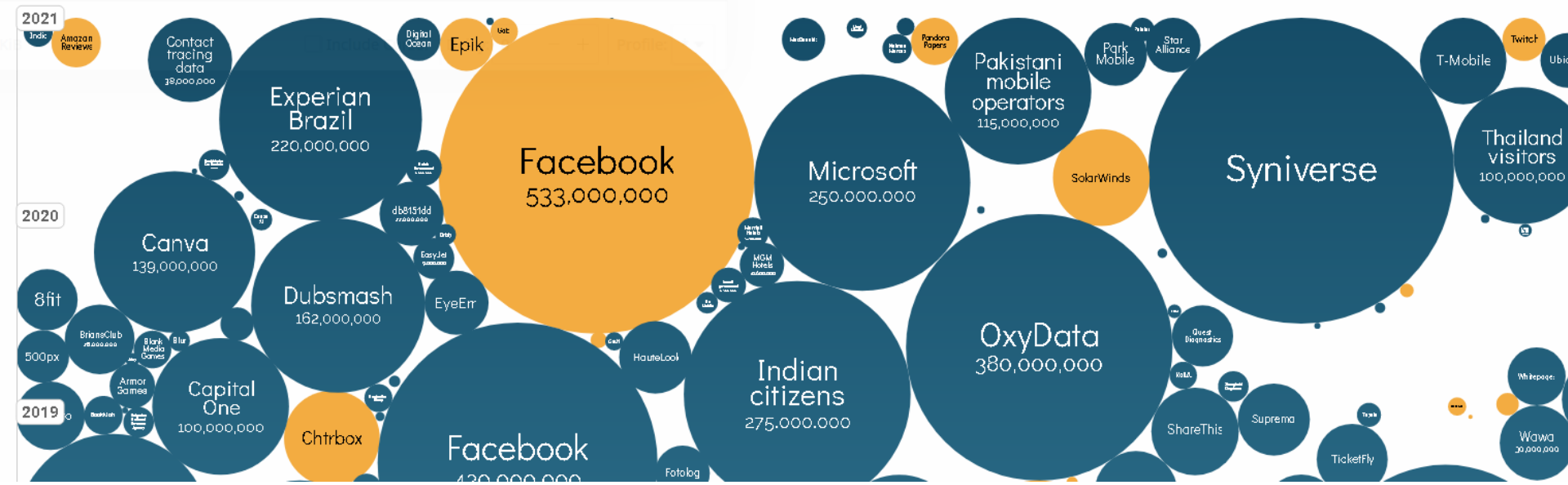
https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

World's Biggest Data Breaches & Hacks

Selected events over 30,000 records

UPDATED: Oct 2021

size: records lost **filter**



https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Recomendación UIT-T X.805

Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo
ITU el grupo de Seguridad en Telecomunicaciones

ISO 18028-2 ISO/IEC 27033-2:2012

UIT-T X.805

Define un marco para analizar la arquitectura y las dimensiones que garantizan la seguridad extremo a extremo de aplicaciones distribuidas.

Los principios y definiciones son válidos para todas las aplicaciones.

Las amenazas y vulnerabilidades y las medidas para contrarrestarlas o minimizarlas dependen de cada aplicación.

Metodología sistemática para analizar la seguridad de una red.

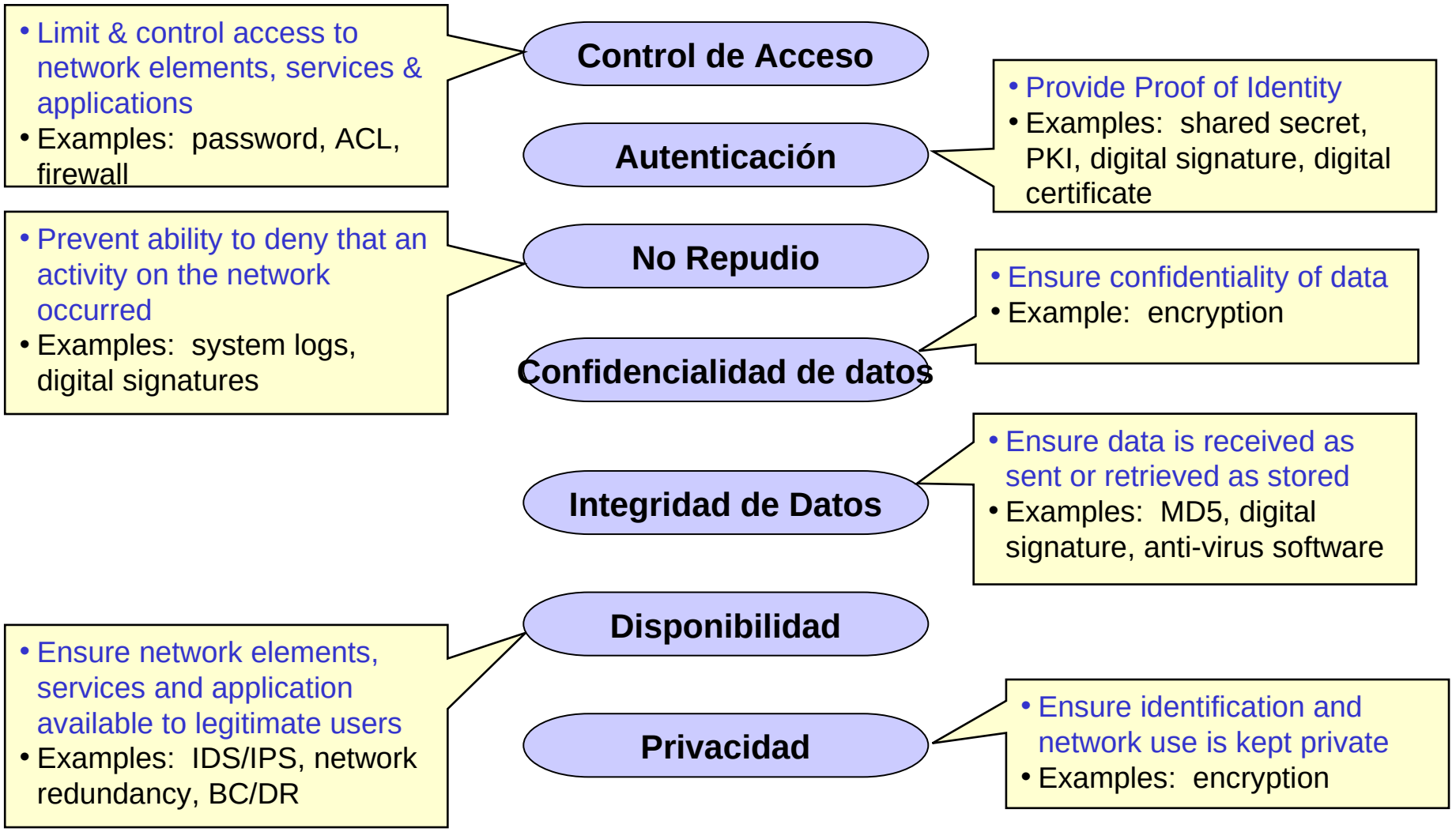
- Define tres capas, tres planos y 8 dimensiones de seguridad

¿Qué protección se quiere y contra qué amenazas?

¿Qué tipos de elementos de infraestructura hay que proteger y de qué manera?

¿Qué actividades en la red hay que proteger?

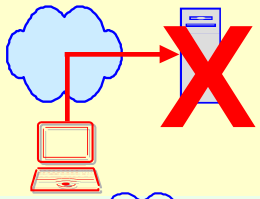
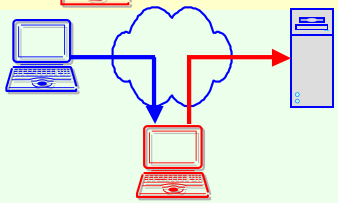
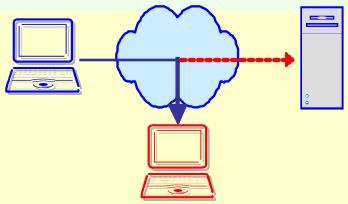
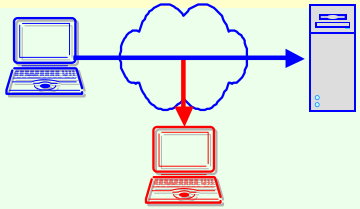
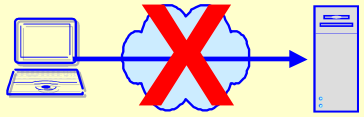
Dimensiones de Seguridad según X805



Dimensiones

- **Autenticación:** Quién pretende acceder a la información o al sistema informático es quien dice ser.
- **Confidencialidad:** Quién pretende acceder a la información o a los sistemas, tiene derecho a hacerlo
- **Integridad:** La información a la que se pretende acceder no ha sido modificada.
- **Disponibilidad:** La información y los sistemas están disponibles cuando se pretende acceder a ellos.
- **Control de Acceso** – prevenir el uso no autorizado de un recurso
- **No Repudio** – No se pueda negar un acto
- **Privacidad** – Confidencialidad de Datos personales.

X.800 Modelo de Amenazas *(simplificado)*

1 - Destrucción Ataque a la ***Disponibilidad***	
2 - Corrupción Ataque a la ***Integridad***:	
3 - Robo Datos Ataque a la ***Disponibilidad***	
4 - Divulgación Ataque a la ***Confidencialidad***	
5 - Interrupción Ataque a la ***Disponibilidad***	

Amenazas

Causa potencial de un incidente no deseado, que puede resultar en daño a un sistema, un individuo o una Organización.

Fuente: ISO 27000 – Cláusula 2.77

Tipos de amenazas

- **AMENAZAS**
  - Naturales
    - Incendios
    - Terremotos
    - Inundacione
  - Humanas
    - Maliciosas
      - Internas
      - Externas
    - No Maliciosas
      - Impericia

fuente ARCERT

Amenazas Externas → **A través de la conexión a Internet**

- ✓ Virus
- ✓ Phishing
- ✓ Spam
- ✓ Troyanos
- ✓ Keyloggers
- ✓ Rootkits
- ✓ Smishing
- ✓ Spyware

→

- ✓ Escaneo de puertos
- ✓ Sabotaje de datos o de red
- ✓ Robo de equipo
- ✓ Software pirata
- ✓ Denegación de servicios
- ✓ Intrusión en la red
- ✓ Fraude financiero
- ✓ Fraude de telecomunicaciones
- ✓ Robo de información protegida por copyright
- ✓ Robo de banda de red wifi
- ✓ Hackeo de sitio web

Las amenazas a través de la Web crecieron en 2006 un 1.300%

Enviar a Amigo Versión impresora

Según el informe Aladdin Malware Report 2006, realizado por la compañía Aladdin Knowledge Systems, el pasado año ha destacado por un crecimiento masivo de troyanos y spyware, mientras que virus y gusanos decrecen considerablemente. En concreto, la compañía asegura que las amenazas a través de la Web han aumentado en un 1.300% en 2006.

Smishing y vishing nuevas amenazas de tipo phishing sobre VoIP y mensajería SMS

ACTUALIDAD

Escrito por Faust

Publicado el 02 de Octubre de 2006 a las 22:10

Amenazas Internas → **Propios usuarios de la red: trabajadores**

No maliciosa →

- ✓ **En 30 días de búsqueda, hay casi un 100% de posibilidades de visitar un sitio peligroso**
- ✓ **97% internautas no sabe detectar programas espía**

Fuente: McAfee

Maliciosa →

- ✓ **81% ataques con el fin de obtener beneficios económicos**
- ✓ **83% en el interior de la organización y durante el horario de trabajo**
- ✓ **22% antiguos empleados**
- ✓ **14% empleados en el momento del ataque**
- ✓ **7% relación cliente o proveedor**

Fuente: Hispasec / Trusted Strategies

Vulnerabilidad

Debilidad de un activo o un control que puede ser explotada por una o varias amenazas.

Fuente: ISO 27000 – Cláusula 2.81

Tipos de Vulnerabilidades

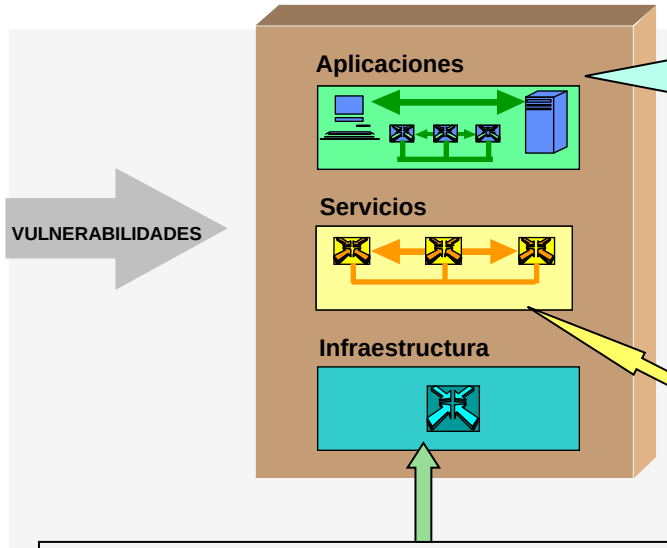
Tipo de Vulnerabilidad	Ejemplos
1 Hardware	Mantenimiento insuficiente
	Portabilidad
2 Software	No hay registros de inscripción
	Interfaces complicadas
3 Red	Falta de encriptación de las transferencias
	Único punto de acceso
4 Personal	Formación insuficiente
	Falte de supervisión
5 Sitio	Sistema eléctrico inestable
	Sitio en un área inundable
6 Estructura de la Organización	Falta de separación de tareas
	No hay descripción de puestos

Fuente: ISO 27005 – Anexo D

Relación entre vulnerabilidad y amenaza

Vulnerabilidad	Amenaza
Almacén desprotegido y sin vigilancia	Robo
Complicados procedimientos de procesamiento de datos	Error en la entrada de datos por parte del personal
No segregación de tareas	Fraude, uso no autorizado de un sistema
Datos no cifrados	Robo de información
Uso de software pirata	virus, perdida de datos
No revisión de los derechos de Acceso	Acceso no autorizado de personas que han abandonado la organización
Procedimientos de backup	Pérdida de información

Capas de Seguridad



3 - Capa de seguridad aplicaciones:

- Ejemplos:
  - Web
  - Email
  - E-commerce
  - …

1 – Capa de seguridad infraestructura:

- Ejemplos:
  - Routers, switches, servers
  - WAN links
  - Ethernet links

2 - Capa de seguridad servicios:

- Ejemplos:
  - IP, DHCP, DNS,AAA
  - VPN
  - VoIP, QoS, Location services

- **Cada capa tiene vulnerabilidades y amenazas propias**
- **Cada capa da soporte de seguridad a la superior.**

Capas de Seguridad

Capa de seguridad infraestructura

- La capa de seguridad infraestructura comprende los dispositivos de transmisión de la red y los elementos de red

Capa de seguridad servicios

- La capa de seguridad servicios tiene que ver con la seguridad de los servicios que los proveedores prestan a sus clientes.

Capa de seguridad aplicaciones

- Tiene que ver con la seguridad de las aplicaciones de red a las que acceden los clientes

Ejemplo: Capas de Seguridad en redes IP

Capa de seguridad infraestructura

- Equipamiento de red: routers, switches y servers
- Links de comunicación.

Capa de seguridad servicios

- Ruteo de la red IP
- Servicios de soporte IP (Ej., AAA, DNS, DHCP)
- Servicios de Valor Agregado: (Ej., VPN, VoIP, QoS)

Capa de seguridad aplicaciones

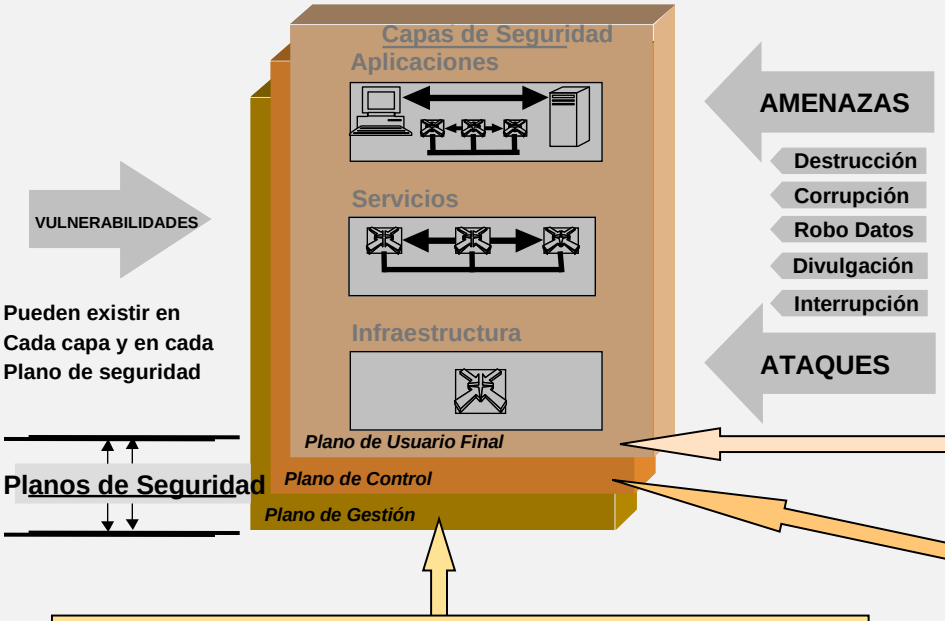
- Aplicaciones de Red Básicas (Ej. FTP, Acceso WEB, File Share)
- Correo, Intranet
- e-commerce,…

Planos de Seguridad

No es lo mismo el patrón característico de uso y las amenazas que pueda tener un usuario que un administrador de seguridad o de sistemas.

Representan los tipos distintos de actividad sobre la red.

Planos de Seguridad



1 – Plano de Usuario Final:

- Acceso y uso de la red y aplicaciones por los usuarios:
  - Conectividad Básica
  - Servicios (VPN, VoIP, etc.)
  - Aplicaciones de Red (correo, Web, ecommerce)

2 – Plano de Control y operación:

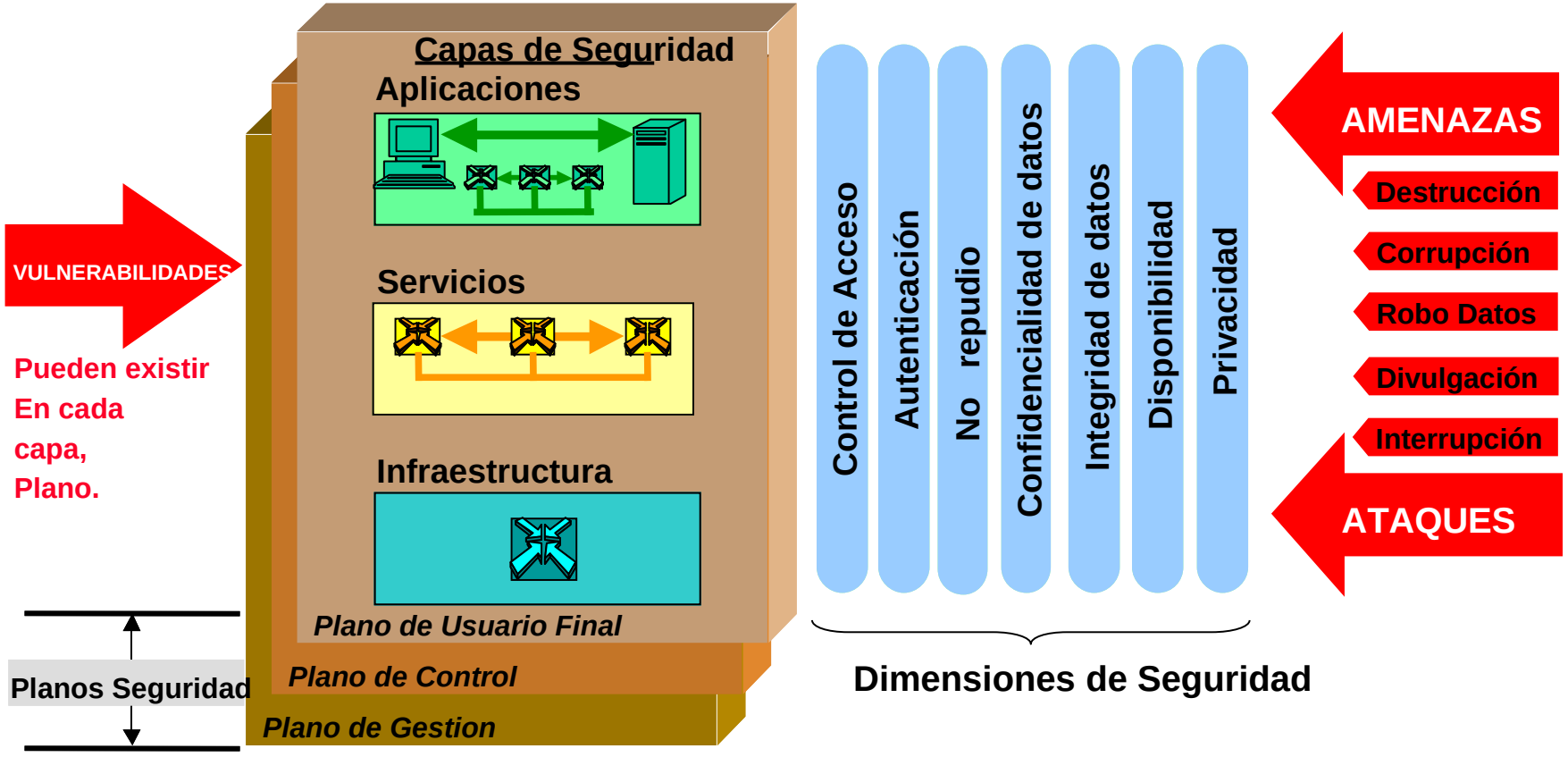
- Actividades para permitir el funcionamiento eficiente de la red

3 – Plano de Gestión:

- Administración de elementos de infraestructura, servicios y aplicaciones.
- FCAPS (Fault, Configuration, Accounting, Performance, Security).
- => anomalía, capacidad, administración, configuración y seguridad.

- **En cada plano de seguridad aplicado sobre cada capa de la seguridad, lo que genera 9 perspectivas.**

ITU-T X.805: Security Architecture for Systems Providing End-to-End Communications



Modular Form of X.805

	Capa Infraestructura	Capa Servicios	Capa Aplicaciones
Plano de Gestion	Modulo uno	Modulo cuatro	Modulo siete
Plano de Control	Modulo dos	Modulo cinco	Modulo ocho
Plano de Usuario	Modulo tres	Modulo seis	Modulo nueve

- Control de Acceso
- Autenticación
- No repudio
- Confidencialidad de datos
- Integridad de datos
- Disponibilidad
- Privacidad

En cada modulo se definen objetivos de control para cada dimensión de seguridad

Objetivos de Seguridad

Módulo 3: Capa infraestructura, plano de usuario	
Dimension seguridad	**Objetivos de seguridad**
Control de acceso	Garantizar que las personas y los dispositivos autorizados son los únicos que pueden acceder a los datos de usuario que transitan por la infraestructura.
Autenticación	Verificar la identidad de la persona o el dispositivo que intentan acceder a los datos de un usuario que transitan por un elemento de la infraestructura.
No repudio	Crear un registro de las personas o dispositivos que han accedido a los datos de usuario que transitan por un elemento de infraestructura. Este registro puede utilizarse como prueba de acceso a los datos de usuario.
Confidencialidad de los datos	Crear un registro de las personas o dispositivos que han accedido a los datos de usuario que transitan por la infraestructura. Este registro puede utilizarse como prueba de acceso a los datos de usuario.
Integridad de los datos	Proteger los datos de usuario que transitan por la infraestructura, contra la modificación, la supresión, la creación y la reactuación sin autorización.
Disponibilidad	Garantizar que nada impedirá que las personas (incluyendo usuarios) y los dispositivos autorizados puedan acceder a los datos de usuario que residen en un dispositivo no conectado. Incluye una protección contra ataques activos, por ejemplo de denegación d
Privacidad	Garantizar que los elementos de red no proporcionan información sobre las actividades del usuario en la red (por ejemplo, la posición geográfica del usuario o los sitios web visitados) a personas o dispositivos no autorizados.

Resumen: X.805 Arquitectura de Seguridad

Puede aplicarse a las políticas y los procedimientos de seguridad, y también a la tecnología, en las tres etapas de un programa de seguridad.

- Definición y Planificación;
- Implementación;
- y Mantenimiento.

Puede ser la base de una evaluación de seguridad, para analizar el efecto del programa de seguridad en las dimensiones, las capas y los planos de seguridad, cuando se realizan las políticas y los procedimientos, y se implanta la tecnología.

Gestión del riesgo

- Vimos
  - Vulnerabilidad
  - Amenaza
  - Ataque
- Vamos a ver
  - Impacto
  - Probabilidad
  - Riesgo = Probabilidad * Impacto
  - Contramedidas o salvaguardas

Activos

Activo: Se denominan activos a los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección.

- Información
- Software
- Hardware
- RRHH

El activo esencial es la información que maneja el sistema; o sea **los datos**.

Impacto

Es el daño producido por la efectivización de una amenaza. Cambio adverso o importante en el nivel de los objetivos de negocios.

Algunos ejemplos

- Confidencialidad:
  - Perdida de imagen publica por fuga de inforación
- Integridad:
  - Problemas legales por perdida de información
- Disponibilidad
  - Perdidas en las ventas por indispoibilidad del sitio de comercio electronico.

¿QUÉ ES EL RIESGO?

Es la Incertidumbre sobre la ocurrencia de un evento que afecte el logro de los objetivos de la organización mediante el siniestro de activos.

- Potencialidad de que una amenaza explote una vulnerabilidad en un activo o grupo de activos y por lo tanto causara daño a la organización.
- Se mide en términos de una combinación de la probabilidad de un evento y sus consecuencias

$$R=PxI$$

Contramedidas o Salvaguardas

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo

- Preventivo
- Detección
- Correctivo

Objetivo de Control y Control

Objetivo de control: Declaración de lo que se quiere lograr como resultado de la aplicación de un control.

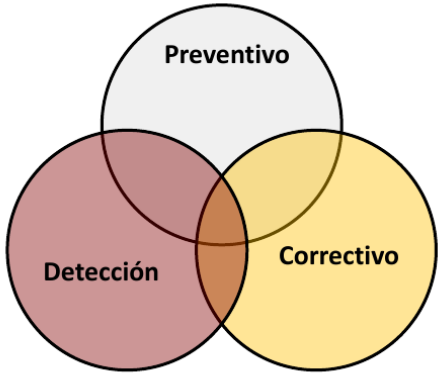
Control: Metodo utilizado para reducir el riesgo. Es un sinonimo de contra medida, salvaguarda o dispositivo de seguridad

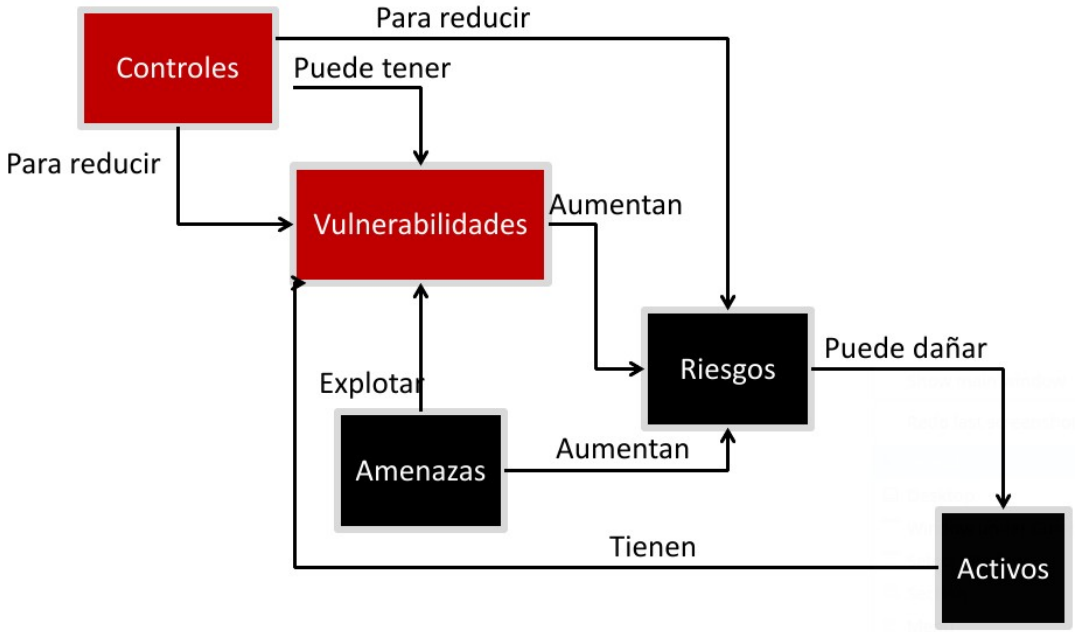
Controles

Control Preventivo: Desalentar o prevenir la aparicion de problemas

Control detectivo: Buscar, detectar e identificar problemas.

Control Correctivo: Resolver problemas




Controles
Para reducir
Puede tener
Para reducir
Vulnerabilidades
Aumentan
Riesgos
Puede dañar
Explotar
Amenazas
Aumentan
Tienen
Activos

Ruyard Kipling The Elephant's Child

I Keep six honest serving-men:
(They taught me all I knew)
Their names are What and Where and When
And How and Why and Who.
I send them over land and sea,
I send them east and west;
But after they have worked for me,
I give them all a rest.

I let them rest from nine till five.
For I am busy then,
As well as breakfast, lunch, and tea,
For they are hungry men:
But different folk have different views:
I know a person small—
She keeps ten million serving-men,
Who get no rest at all!
She sends ‘em abroad on her own affairs,
From the second she opens her eyes—
One million Hows, two million Wheres,
And seven million Whys!

Mantengo seis servidores honestos:
(Me enseñaron todo lo que sabía)
Sus nombres son Qué, Dónde y Cuándo.
Y cómo, por qué y quién.
Los envío por tierra y mar,
Los envío al oriente y al occidente;
Pero después de que hayan funcionado para mí,
Les doy un descanso a todos.

Los dejé reposar de nueve a cinco.
Porque estoy ocupado entonces,
Además del desayuno, el almuerzo y el té,
Porque son hombres hambrientos:
Pero diferentes personas tienen diferentes puntos de vista:
Conozco a una persona pequeña
Ella mantiene diez millones de sirvientes,
¡Que no descansan en absoluto!
Los envía al extranjero por sus propios asuntos,
Desde el momento en que abre los ojos...
Un millón de cómo, dos millones de dónde,
¡Y siete millones de porqués!

Dos recursos fundamentales

- **Las 6 W** (o sea: las seis doblevés, porque se definieron a partir de la escuela norteamericana)

  - **Who – Quién**
  - **Wath - Qué**
  - **When – Cuándo**
  - **Where – Dónde**
  - **Why – Por qué /**
  - **How – Cómo**

- **La pirámide invertida**
  (o sea, un triángulo con la punta para abajo y la base para arriba).

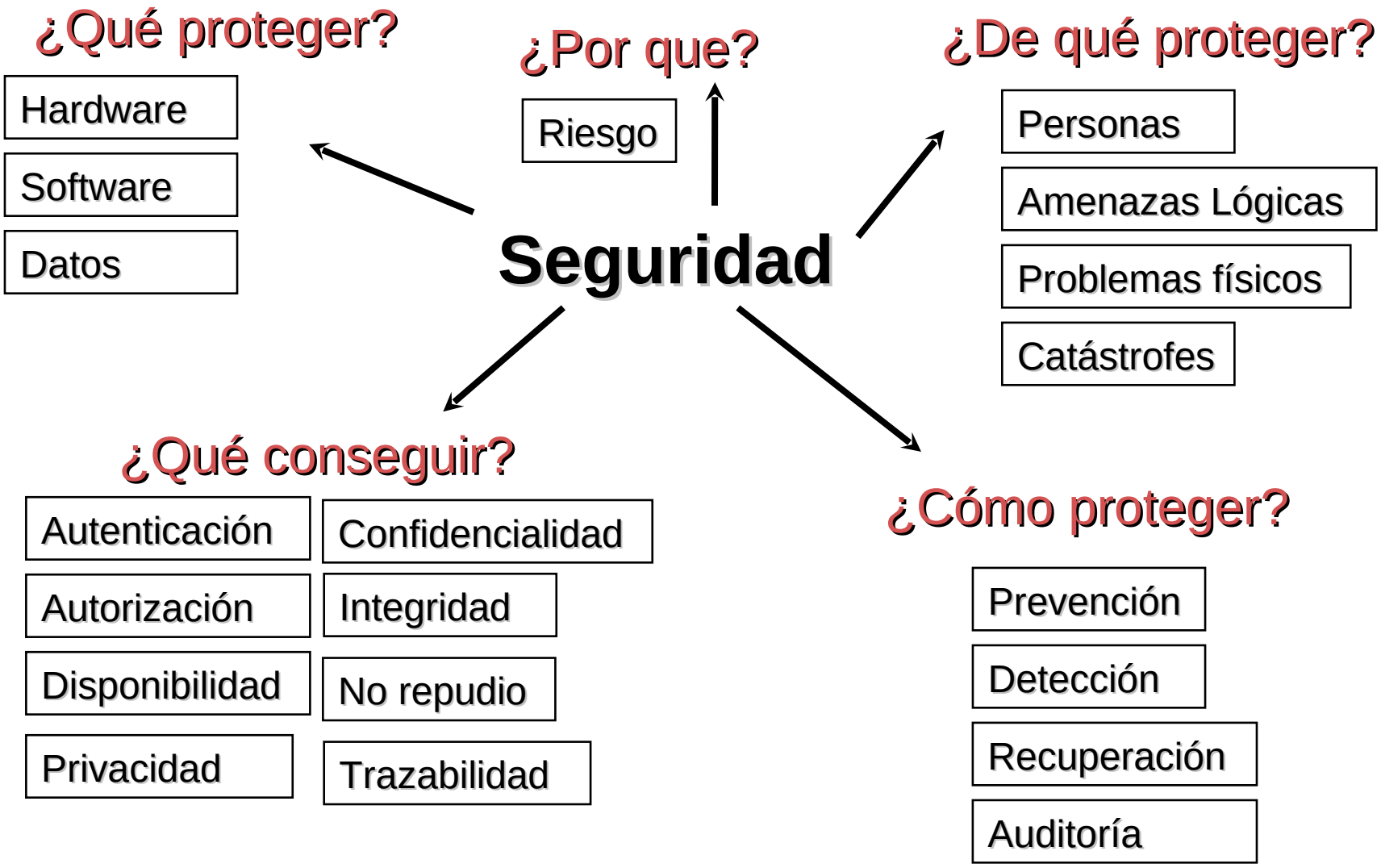
  - **(eso lo veremos luego)**

Las 6 W

- **QUÉ:**
  - *¿Qué sucedió?*
- **QUIÉN:**
  - *¿Quién es el protagonista de esta noticia?*
  - *¿Quién está involucrado en esta historia?*
- **DÓNDE:**
  - *¿Dónde sucedió esto? ¿En que lugar? Calle, barrio, ciudad. Departamento, casa, calle, aeropuerto, oficina de trabajo, organismo público.*
- **CUÁNDO:**
  - *¿Cuándo sucedió esto?*
  - *¿Cuándo tuvieron lugar los momentos decisivos de esta historia?*
- **CÓMO**:
  - *¿Cómo ocurrió esto? ¿Qué circunstancias lo hacen particular, distintivo, único? ¿Es una modalidad frecuente?*
- **POR QUÉ:**
  - *¿Por qué ocurrió esto? ¿Es un caso aislado o forma parte de una tendencia?*

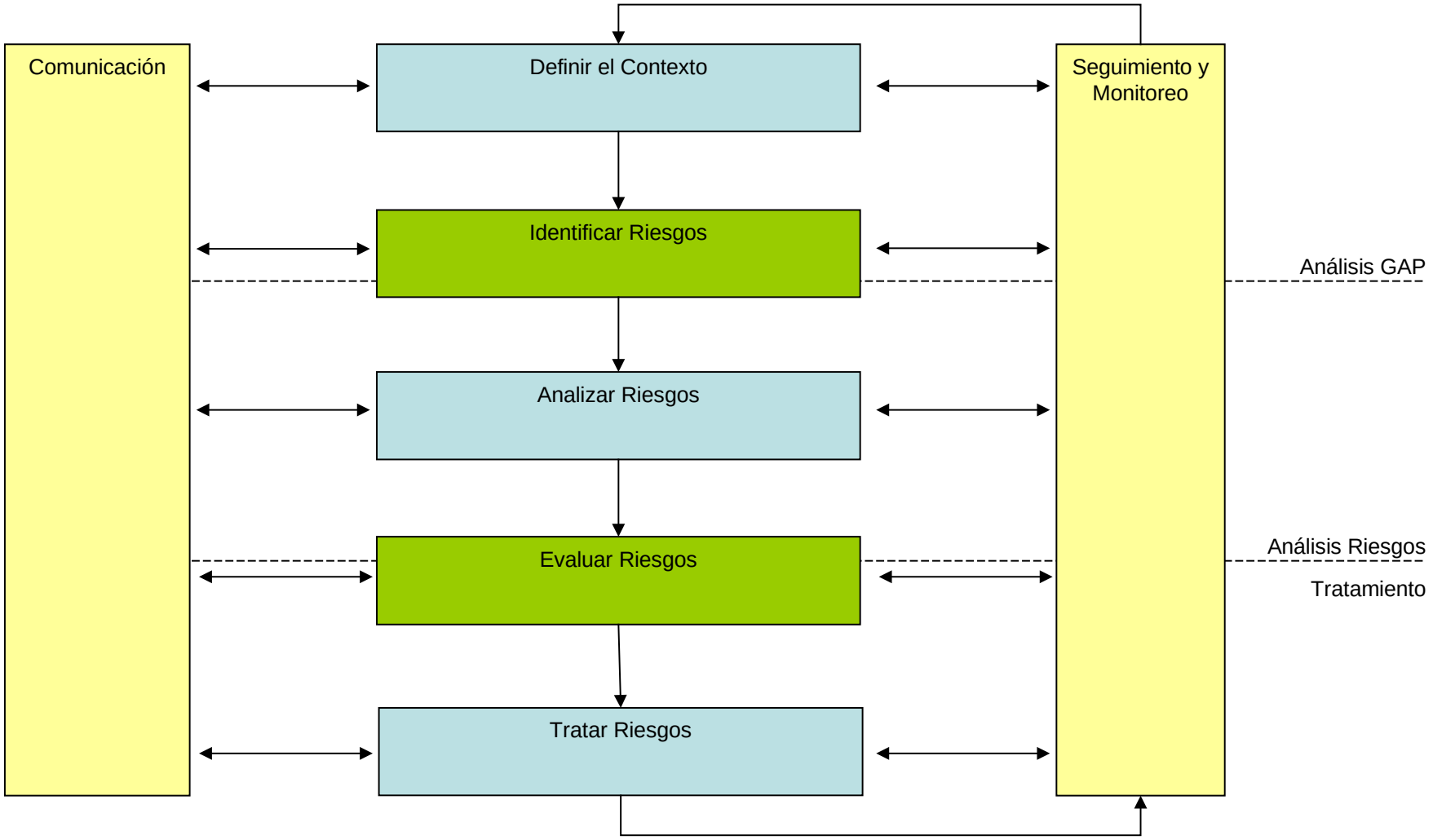
Pilares de la seguridad

- Qué debe ser protegido?
- Por qué debe ser protegido?
- De qué debe ser protegido?
- Cómo protegerlo?


¿Qué proteger?
Hardware
Software
Datos
¿Por que?
Riesgo
¿De qué proteger?
Personas
Amenazas Lógicas
Problemas físicos
Catástrofes
Seguridad
¿Qué conseguir?
Autenticación
Confidencialidad
Autorización
Integridad
Disponibilidad
No repudio
Privacidad
Trazabilidad
¿Cómo proteger?
Prevención
Detección
Recuperación
Auditoría

- Administración del riesgo - Estrategia Reactiva
- Administración del riesgo - Estrategia Proactiva
  - Se identifican los riesgos potenciales, se valoran su probabilidad y su impacto y se establece una prioridad según su importancia

Gestión del Riesgo



Fase 1 Definir el alcance

Por ejemplo sobre

- Los procesos del departamento Administración,
- Los procesos de producción y gestión de almacén
- Los sistemas TIC relacionados con la página web de la empresa, etc.
- Los servicios y sistemas del Departamento Informática”.

https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

Fase 2 Identificar los Activos

- Listar los activos involucrados en el proceso o servicio bajo analisis.
- Tecnología: Aplicaciones, Bases de datos, Computadoras, correo electrónico, Memorias USB, infraestructura de red, etc
- Documentos Impresos: Planillas, publicaciones, etc
- Gente

Fase 3 Identificar las amenazas

- Determinar las amenazas que pueden afectar a cada activo.
- Las amenazas son “cosas que ocurren”. Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño
  - Determinar el impacto o la degradación
  - Determinar la frecuencia o probabilidad de ocurrencia

Fase 3 Identificar las amenazas

[N] DESASTRES NATURALES Pueden ocurrir sin intervención de los seres humanos	
Fuego	Incendios, posibilidad de que el fuego acabe con recursos del sistema.
Daños por agua	Inundaciones, posibilidad de que el agua acabe con recursos del sistema

[I] DE ORIGEN INDUSTRIAL Pueden ocurrir en forma accidental, derivados de la actividad humana	
Avería de origen físico o lógico	Fallos en los equipos y/o programas.
Corte de suministro eléctrico	Cese de la alimentación de potencia.
Fallo de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro.
Degradación de los soportes de almacenamiento de información	Como consecuencia del paso del tiempo

Fase 3 Identificar las amenazas

[E] ERRORES Y FALLOS NO INTENCIONADOS	
Errores de usuarios	Equivocaciones de las personas.
Errores de monitorización (logs)	Inadecuado registro de actividades.
Difusión de software dañino	Propagación inocente de virus, espías
Deficiencias en la organización	Cuando no está claro quien tiene que hacer exactamente que y cuando.

[A] ATAQUES INTENCIONADOS	
Uso no previsto	Utilización de los recursos del sistema para fines no previstos: juegos, etc.
Acceso no autorizado	El atacante consigue acceder a los recursos del sistemas sin tener autorización para ellos
Ataque destructivo	Vandalismo, terrorismo etc.

Fase 4 Identificar salvaguardas

- Busqueda de salvaguardas a las amenazas identificadas
  - Hay amenazas que se conjuran simplemente organizándose adecuadamente,
  - Otras requieren elementos técnicos (programas o equipos), ejemplo: Firewall
  - Otras seguridad física. Ej.: Control de accesos.
  - Política de personal.
- Se busca
  - Reducir la frecuencia
  - o limitar el daño causado (Impacto)

Fase 5 Evaluar el riesgo

Analisis del impacto derivado de la materialización de una amenaza.

- **Disponibilidad** ¿Qué importancia tendría que el activo no estuviera disponible?
- **Integridad** ¿Qué importancia tendría que el activo fuera modificado sin permiso?
- **Confidencialidad** ¿Qué importancia tendría que el activo fuera conocido por personas no autorizadas?

Fase 5 Evaluar el riesgo

Tabla para calculo de la probabilidad

Cualitativo	Cuantitativo	Descripción
Baja	1	La amenaza se puede materializar en un año
Media	2	una vez por mes
Alta	3	cada semana
Muy Alta	4	diariamente

Tabla para calculo del impacto

Cualitativo	Cuantitativo	Descripción
Muy Bajo	1	el daño no tiene consecuencias relevantes
Bajo	2	el daño tiene consecuencias
Medio	3	el daño tiene consecuencias importantes
Alto	4	El daño tiene consecuencias graves
Muy Alto	5	El daño tiene consecuencias muy graves

Fase 5 Evaluar el riesgo

El riesgo crece con el impacto y con la frecuencia.

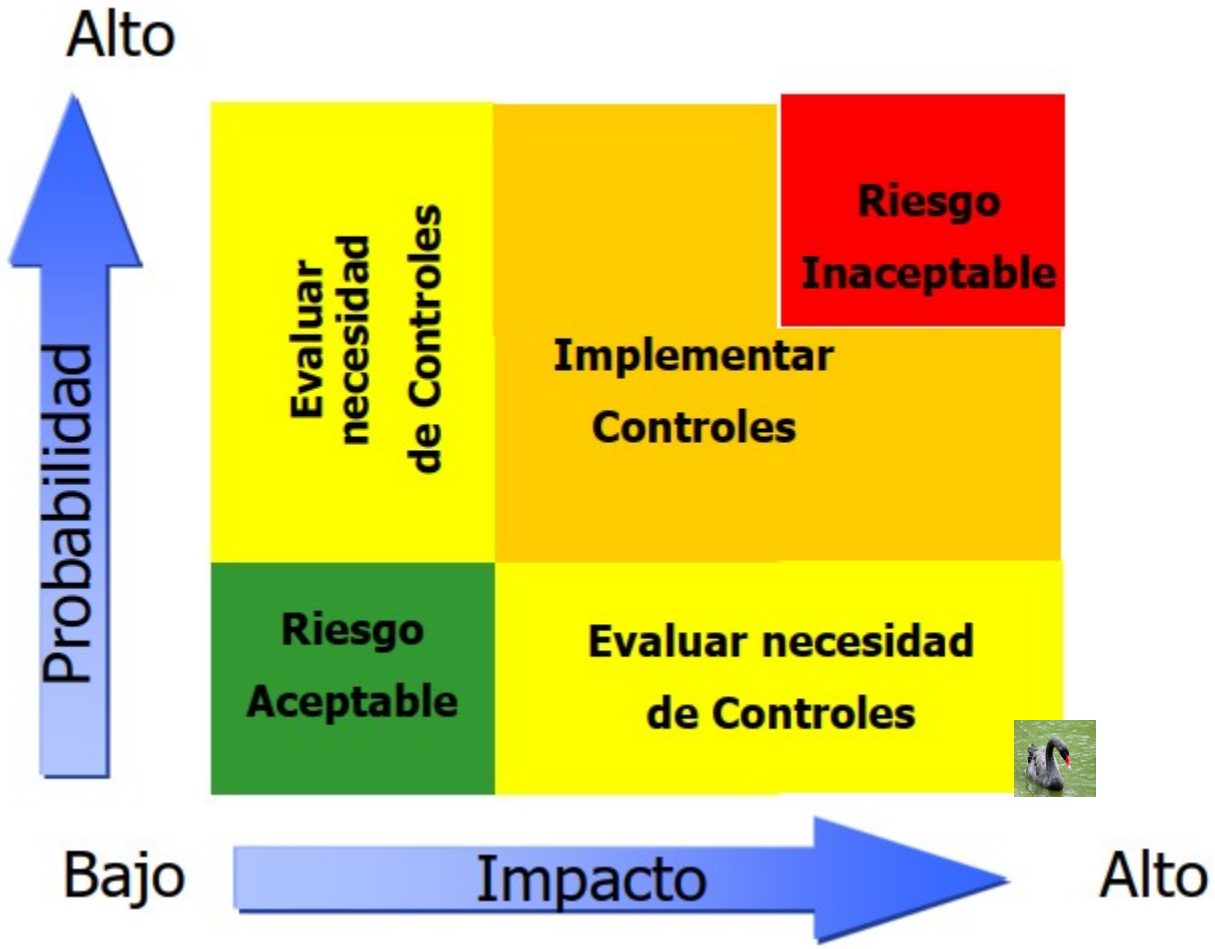
Probabilidad	Nivel de Impacto				
	1. Muy Bajo	2. Bajo	3. Medio	4. Alto	5. Muy Alto
5. Muy Alta	H	H	E	E	E
4. Alta	M	H	H	E	E
3. Media	L	M	H	E	E
2. Baja	L	L	M	H	E
1. Muy Baja	L	L	M	H	H

Criticidad:

E	Extremo
H	Alto
M	Medio
L	Bajo

- **Evaluados los activos, las amenazas, la probabilidad de ocurrencia de los riesgos y el nivel del impacto en el sistema de información.**
- **Dependiendo del "Apetito del Riesgo" de la organización, la matriz nos da las prioridades de inversión en seguridad informática (señalados en rojo o en amarillo)**

Fase 5 Evaluar el riesgo

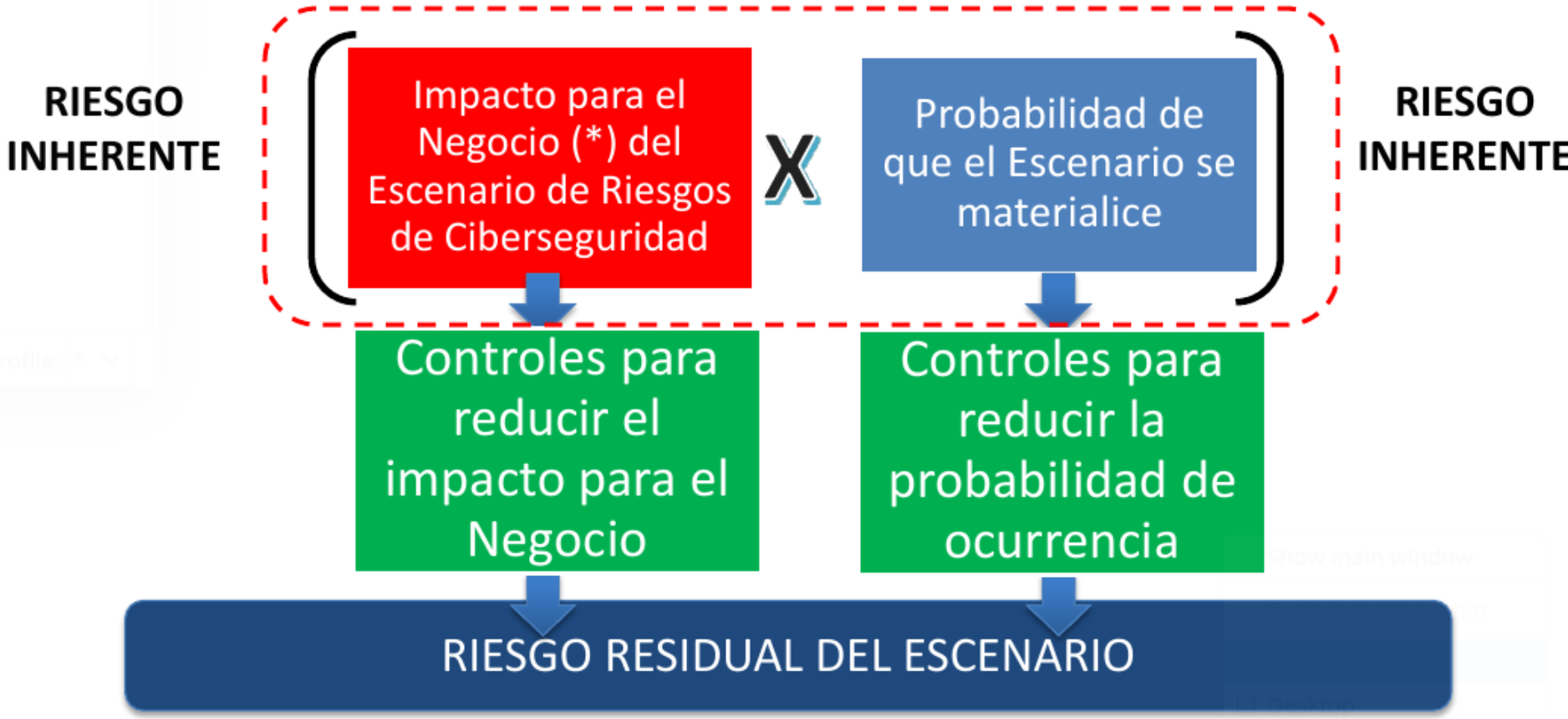


Fase 6 Tratamiento del Riesgo

Estrategias básicas

- **Transferir**: Contratos con terceros o seguros
- **Aceptar**: Inversión en seguridad sobrepasa las perdidas
- **Eliminar** la exposición
- **Reducir o mitigar**: Implementando controles

Riesgo inherente vs riesgo residual



Cisne Negro

Probabilidad muy baja con impacto muy alto


PROPIETARIO INFORMACIÓN
define
CRITICIDAD ACTIVOS
+
IMPACTO EN NEGOCIO
ANÁLISIS DE RIESGOS
COORDINADO
+
CONSENSUADO
RESPONSABLE SEGURIDAD
diseña e implementa
CLASIFICACIÓN INFORMACIÓN
+
MEDIDAS DE SEGURIDAD

Actividad

- Fase 1 Definir el alcance
- Fase 2 Identificar los Activos.
- Fase 3 Identificar las amenazas
    - Conjunto de amenazas a las que está expuesta cada activo.
    - Conjunto de vulnerabilidades asociadas a cada activo (si corresponde).
- Fase 4 Identificar salvaguardas
- Fase 5 Evaluar el riesgo
    - Determinación de la Probabilidad
    - Determinación del impacto
    - Calculo del riesgo
- Fase 6 Tratamiento del Riesgo
    - Transferir
    - Aceptar
    - Eliminar
    - Mitigar

como sera la materia?

Algunos enlaces

https://owasp.org/

https://owasp.org/www-project-top-ten/

https://www.nist.gov/cyberframework

https://www.sans.org/top25-software-errors/

https://cve.mitre.org/ vulns

https://www.nist.gov/itl/current-fips

sp800 https://csrc.nist.gov/publications/sp

https://www.elladodelmal.com/ Blog de Chema

https://www.dragonjar.org/ Comunidad

https://seguridadyredes.wordpress.com/

https://hispasec.com/es/ (autores de una al día)