SEGURIDAD DE LA INFORMACIÓN

TEMA 1

FUNDAMENTOS DE SEGURIDAD

Índice del tema

- Introducción
  - Seguridad de la Información: Conceptos
  - Ciclo de vida de la Seguridad
  - Modelo de escenario de Seguridad,
    - Ataques principales
- Servicios y mecanismos de seguridad
  - Las cinco categorías fundamentales:
    - C - confidencialidad
    - I - integridad
    - A - autenticación
    - A – (control de acceso) - autorización
    - N – no repudio
  - La jerarquía: Servicios, Protocolos, Mecanismos, Técnicas

INTRODUCCIÓN

- Algunas definiciones de "Seguridad de la Información"

*"Information security is the **protection of information from a wide range of threats** in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities"*

ISO/IEC 17799: Code of practice for information security management

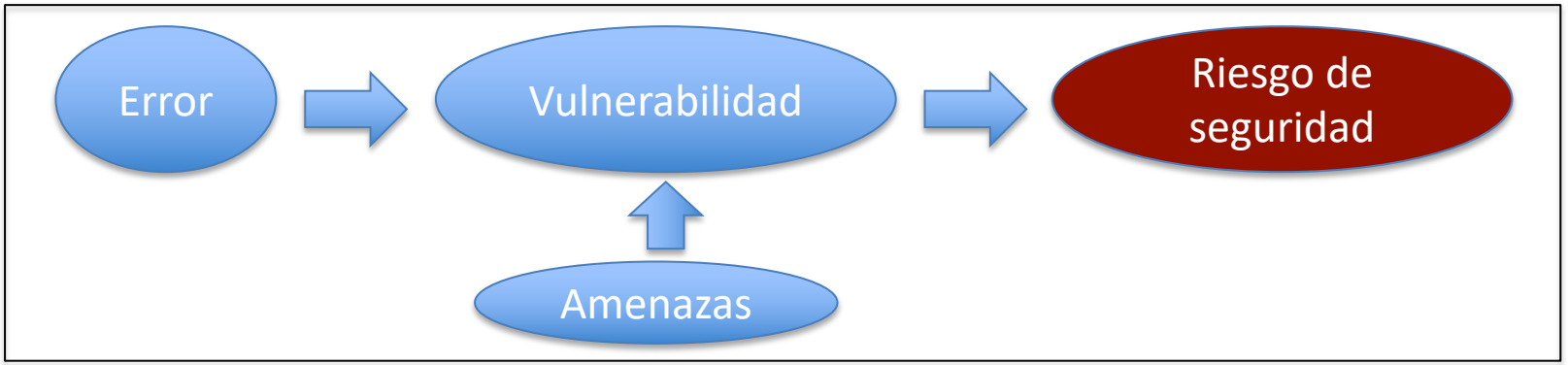
*"The **protection of information assets** through the use of technology, processes, and training"*

Microsoft Security Glossary

*"The ability of a system to **manage, protect, and distribute sensitive information**"*

Software Engineering Institute, Carnegie Mellon University

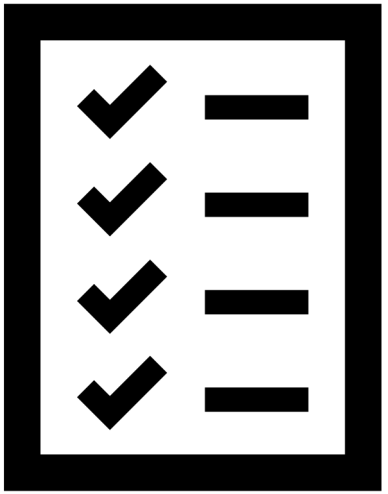
- Un error en la fase de análisis, diseño, desarrollo o implementación puede producir, a posteriori, un fallo de seguridad
  - También llamado vulnerabilidad



- Como consecuencia, se viola la política de seguridad del sistema, y este queda en peligro
  - En una red como Internet, con las dimensiones, números de hosts y número de usuarios actuales, el efecto devastador es exponencial

Ciclo de vida de la Seguridad

- La política de seguridad es el conjunto de reglas/requisitos que gobiernan el comportamiento del sistema, en lo que a seguridad se refiere
- Ejemplos de requisitos:
  - mantener la información en secreto, salvo para quienes están autorizados a verla
  - garantizar que la información no ha sido alterada por amenazas autorizadas o desconocidas
  - garantizar siempre el acuse de recibo de la información (ACK) recibida
  - verificar la creación o existencia de información por una entidad distinta de su creador
  - ocultar la identidad de una entidad implicada en algunos procesos
  - Prevenir la denegación de compromisos previos o acciones
  - Etc.

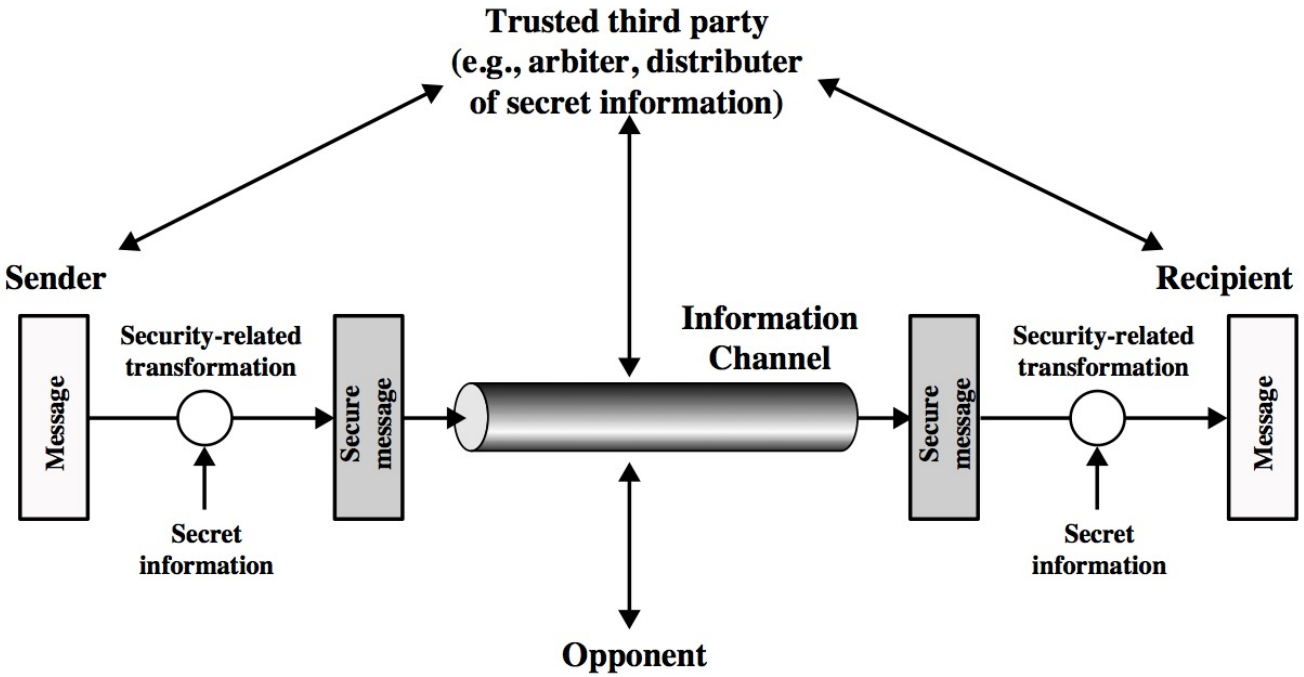


- La política de seguridad es sólo una de las fases del ciclo de vida de la seguridad.
- El modelo general de ciclo de vida se incluye en el estándar ISO-7498-2, y consta de cinco pasos:

1. Definición de una política de seguridad que contiene una serie de requisitos "genéricos" de seguridad para el sistema
2. Análisis de requisitos de seguridad, incluyendo el análisis de riesgos, y un análisis de los requisitos legales, gubernamentales y normativos
3. Definición de los servicios de seguridad necesarios para satisfacer los requisitos de seguridad
4. Diseño del sistema e implementación, así como la selección de los mecanismos de seguridad que van a proporcionarnos los servicios de seguridad definidos en la etapa anterior
5. Administración y mantenimiento de la seguridad

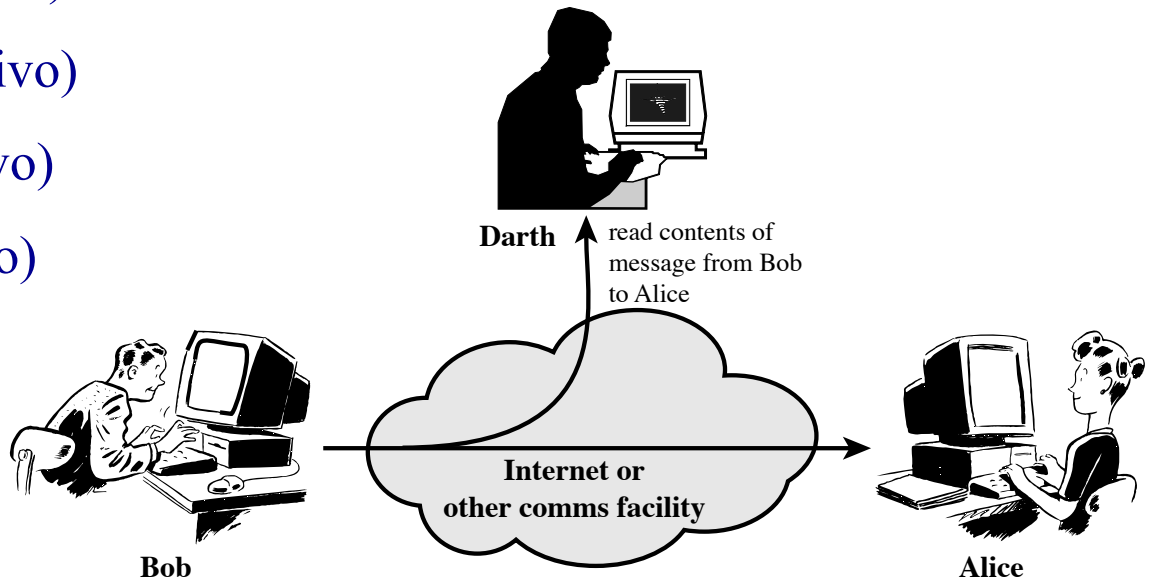
Modelo de escenario de Seguridad

- Es necesario un escenario básico para empezar a razonar sobre:
  - las amenazas que pueden existir y los ataques que se pueden sufrir
  - las soluciones (servicios y mecanismos) de seguridad que podemos utilizar

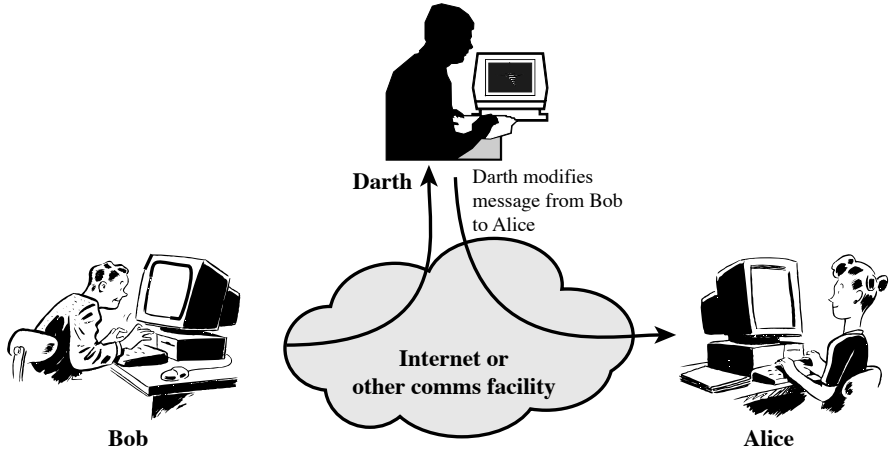


- ¿Quiénes pueden ser el emisor y el receptor en un escenario real?
  - Navegador web y Servidor web para transacciones electrónicas (por ejemplo, compra on-line)
  - Banca on-line (cliente y servidor)
  - Servidores DNS
  - Routers intercambiando tablas de enrutamiento
  - Dos usuarios en un chat, o enviándose e-mails, …
  - Etc.

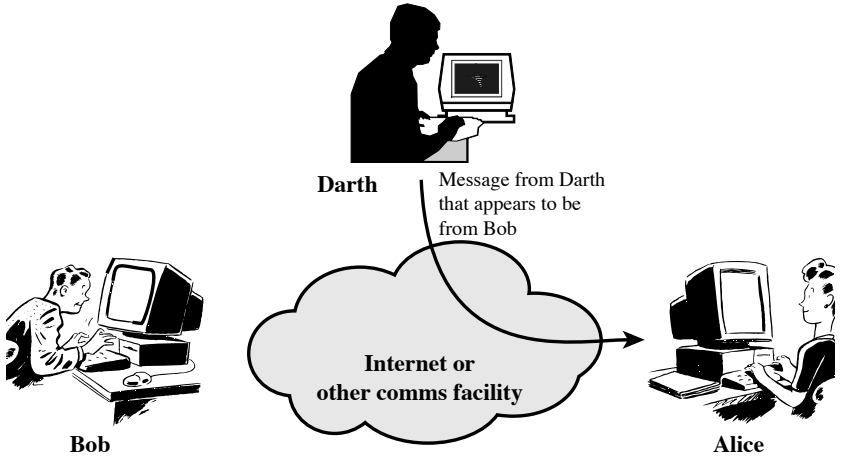
- Los ataques se pueden clasificar en activos y pasivos
- Más concretamente, se pueden considerar los siguientes cuatro tipos:
  - Intercepción (pasivo)
  - Modificación (activo)
  - Interrupción (activo)
  - Generación (activo)



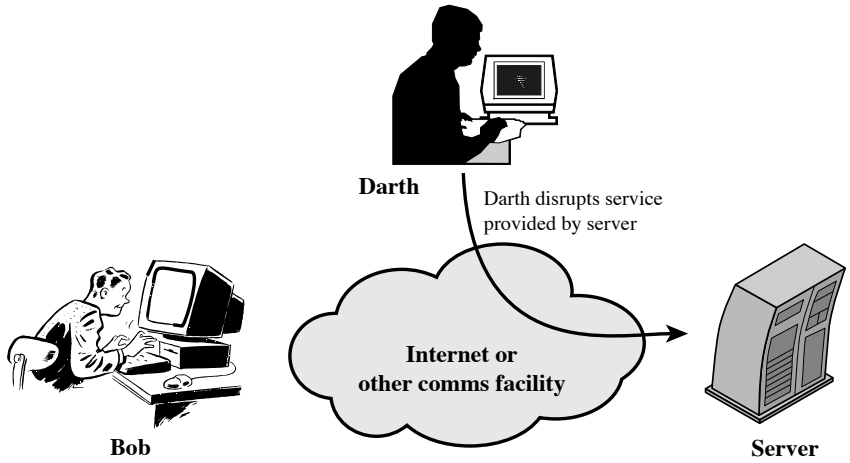
Intercepción



Modificación



Generación



Interrupción

SERVICIOS Y MECANISMOS DE SEGURIDAD

- Los servicios de seguridad ponen en funcionamiento las políticas de seguridad
- Algunas definiciones más precisas para este concepto:

*"A **processing or communication service** that is provided by a system **to give a specific kind of protection** to system resources"*

RFC 2828: Internet Security Glossary

*"A service, provided by a layer of communicating open systems, which **ensures adequate security of the systems or the data transfers"***

ISO 7498-2: Basic Reference Model -- Part 2: Security Architecture

ITU X.800: Security Architecture for Open Systems Interconnection for CCITT Applications

- Los estándares ISO 7498-2 e ITU X.800 dividen los servicios de seguridad en **cinco categorías**, y a partir de ahí distinguen **catorce servicios específicos**
- Las categorías son:
  - Confidencialidad de datos
  - Autenticación (de usuarios y de datos)
  - Integridad de datos
  - No-repudio (de origen y destino)
  - Control de acceso (autorización)
- A continuación, vamos a ver algunas definiciones dada por el National Institute of Standards and Technology (NIST) en https://csrc.nist.gov/glossary/

Confidencialidad

- **Preservar el acceso autorizado y divulgación de la información**, incluidos los medios para proteger la intimidad personal y la información sujeta a derechos de propiedad
- Se usa este servicio cuando no deseo que otros usuarios conozcan:
  - mis e-mails que envío, o chats
  - mi DNI o número de la Seg. Social
  - mi número de tarjeta de crédito
  - mis datos médicos
  - las webs que visito, lo que compro y dónde viajo
  - mi salario
  - lo que voto
  - Etc.

- Otros ejemplos:
  - Coca-Cola no desea que se conozca su fórmula
  - Las empresas quieren proteger sus tecnologías
  - Los gobiernos quieren mantener en secreto sus planes

- La confidencialidad puede aplicarse a un dato concreto a un conjunto de datos

Auntenticación

- **Verificación de la identidad de un usuario, proceso o dispositivo,** a menudo como requisito previo para permitir el acceso a los recursos de un sistema de información
- Se usa este servicio cuando quiero estar seguro de que las entidades con las que interactúo "*son quienes dicen ser*":
  - mi amiga Alicie
  - mi médico
  - Amazon
  - …
- Es decir, quiero tener garantías que nadie está suplantando la identidad de mi interlocutor
- La autenticación puede aplicarse a nivel de usuario o a nivel de datos

Integridad

- **Protección contra la modificación o destrucción indebida de la información,** e incluye garantizar el no repudio y la autenticidad de la información
- Se usa este servicio cuando no deseo que:
  - los mails o chats que envío o recibo sean modificados o falsificados
  - alguien borre (conscientemente o no) una parte de mis registros médicos
  - se puedan falsificar las órdenes que envío a mi banco para realizar pagos/cobros
  - alguien puede modificar mi declaración de Hacienda cuando la relleno/envío por la Web
  - etc.
- La integridad puede aplicarse puede aplicarse a un dato concreto a un conjunto de datos

No repudio

- **Dar garantías de que el remitente de la información dispone de una prueba de entrega y el destinatario de una prueba de la identidad del remitente, de modo que ninguno de los dos pueda "negar" posteriormente haber procesado la información**
  - No repudio de origen: el destino tiene una prueba de que el mensaje fue enviado por la entidad especificada
  - No repudio de destino: el origen tiene una prueba de que el mensaje fue recibido por la entidad especificada
- Se usa este servicio cuando deseo:
  - tener pruebas de que ha ocurrido cierto evento:
  - tener pruebas del instante exacto en que ha tenido lugar ese evento
  - tener pruebas de qué entidades han intervenido en el evento
  - conocer cualquier información adicional específicamente asociada al evento

Control de acceso (autorización)

- **El proceso de concesión o denegación de solicitudes específicas para obtener y utilizar información y servicios** relacionados con el tratamiento de la información; y para entrar en instalaciones físicas específicas
- Se usa este servicio cuando deseo:
  - permitir el acceso a mis recursos a usuarios autorizados
  - denegar el acceso a mis recursos a usuarios desconocidos
  - limitar y monitorizar el uso de ciertos recursos
  - definir reglas de acceso
  - garantizar el uso de credenciales correctos de acceso
  - Etc.

- Dentro de una comunicación, estos servicios de seguridad se pueden proporcionar en distintas capas del modelo de referencia OSI, como indica la siguiente tabla:

Service / Layer	Layer 1	Layer 2	Layer 3	Layer 4	Layer 5/6	Layer 7
Entity authentication			Y	Y		Y
Origin authentication			Y	Y		Y
Access control			Y	Y		Y
Connection confidentiality	Y	Y	Y	Y		Y
Connectionless confidentiality		Y	Y	Y		Y
Selective field confidentiality						Y
Traffic flow confidentiality	Y		Y			Y
Connection integrity with recovery				Y		Y
Connection integrity without recovery			Y	Y		Y
Selective field connection integrity						Y
Connectionless integrity			Y	Y		Y
Selective field connectionless integrity						Y
Non-repudiation of origin						Y
Non-repudiation of delivery						Y

- Por otro lado, un mecanismo de seguridad proporciona soporte a un servicio de seguridad
- Definición:

> *"A process (or a device incorporating such a process) that can be used in a system to **implement a security service** that is provided by or within the system"*
>
> RFC 2828: Internet Security Glossary

- Los estándares ISO 7498-2 e ITU X.800 distinguen entre dos tipos de mecanismos de seguridad:
  - ***específicos***: están implementados en una capa específica de la pila de protocolos
  - ***ubicuos***: no son específicos de ninguna capa en particular

ESPECÍFICOS	UBÍCUOS
Cifrado	**Controles de seguridad**
Firma digital	**Etiqueta de seguridad**
Control de acceso	**Certification, validación, simulación**
Integridad del dato	**Detección y prevención de eventos**
Autenticación	**Auditoría y accountability**
Padding	**Recuperación de la seguridad**
Control de enrutamiento	**Forense**
Tercera persona de confianza (Trusted Thrid Party)	**Gestión de la confianza, reputación**
	…

Service \ Mechanism	Encipherment	Digital signature	Acces control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y	·	·	Y	·	·	·
Data origin authentication	Y	Y	·	·	·	·	·	·
Access control service	·	·	Y	·	·	·	·	·
Connection confidentiality	Y	.	·	·	·	·	Y	·
Connectionless confidentiality	Y	·	·	·	·	·	Y	·
Selective field confidentiality	Y	·	·	·	·	·	·	·
Traffic flow confidentiality	Y	·	·	·	·	Y	Y	·
Connection Integrity with recovery	Y	·	·	Y	·	·	·	·
Connection integrity without recovery	Y	·	·	Y	·	·	·	·
Selective field connection integrity	Y	·	·	Y	·	·	·	·
Connectionless integrity	Y	Y	·	Y	·	·	·	·
Selective field connectionless integrity	Y	Y	·	Y	·	·	·	·
Non-repudiation. Origin	·	Y	·	Y	·	·	·	Y
Non-repudiation. Delivery	·	Y	·	Y	·	·	·	Y

· The mechanism is considered not to be appropriate.

Y Yes: the mechanism is considered to be appropiate, either on its own or in combination with other mechanisms.

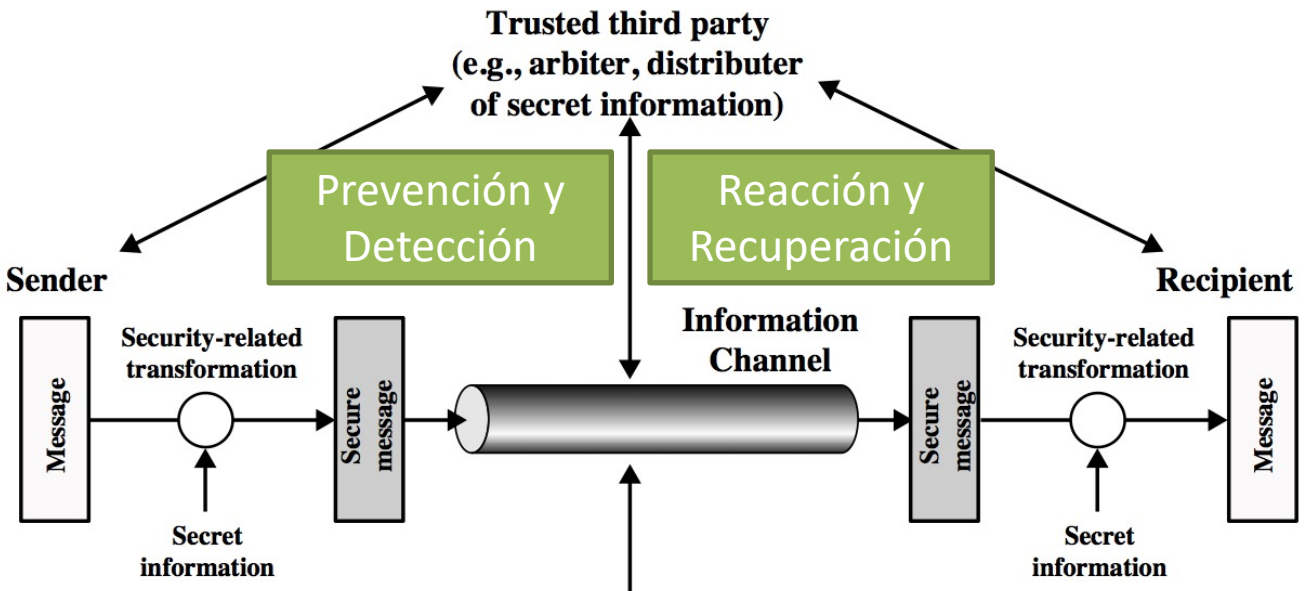
Note – In some instances, the mechanism provides more than is necessary for the relevant service but could nevertheless be used.

- Resumiendo, un servicio de seguridad está basado de:
  - Un protocolo de seguridad* (opcional) es un conjunto de reglas y formatos que determinan la información que se intercambian dos (o más) entidades con objeto de proporcionar un servicio de seguridad
  - Los mecanismos de seguridad son las piezas básicas con las que se construyen protocolos de seguridad
  - Los mecanismos de seguridad se apoyan en técnicas criptográficas

El ecosistema de la Seguridad

Distintas dimensiones de la seguridad

Esquemas de certificación / testeo



Requisitos y Riesgos

Diseño seguro / privado

Mecanismos de protección

RED TEAM

BLUE TEAM

PURPLE TEAM

Análisis Forense

¿Cuáles son las salidas profesionales de la ciberseguridad?

https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework

¿Quién define los estándares / buenas prácticas?

- Organizaciones de estandarización
  - ISO/IEC (International Organization for Standardization / International Electrotechnical Commission)
    - ISO/IEC JTC 1 – Joint technical committee on information technology
  - ETSI (European Telecommunications Standards Institute)

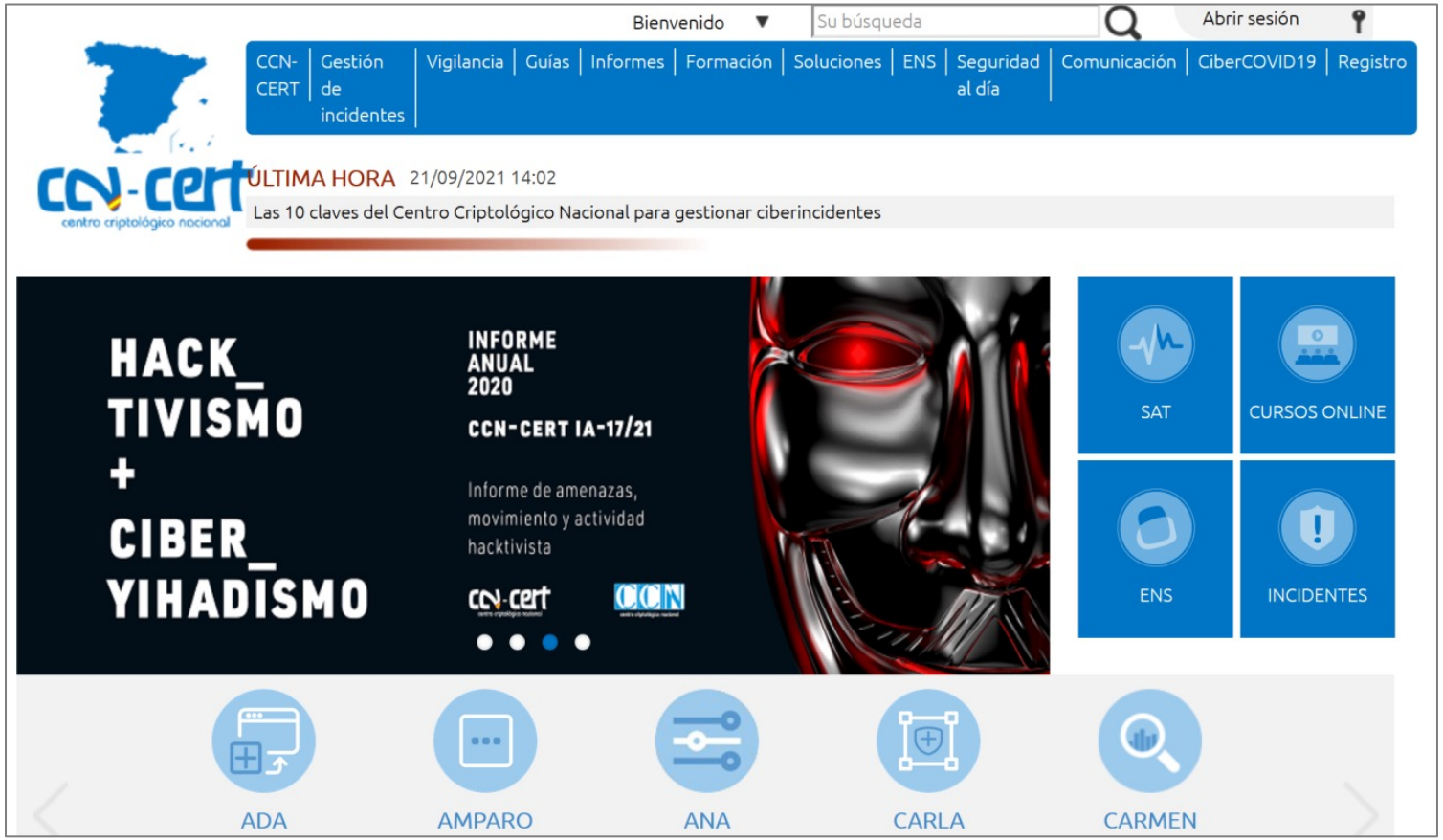
- Diversos gobiernos, alianzas, etc.
  - NIST (National Institute of Standards and Technology)
  - ENISA (EU Agency for Cybersecurity)

¿Qué organizaciones españolas tratan la ciberseguridad?

- INCIBE – Instituto Nacional de Ciberseguridad
  - Para las empresas y los ciudadanos

¿Qué organizaciones españolas tratan la ciberseguridad?

- CCN-CERT
  - Para las empresas públicas, organismos del estado, y otras empresas



Referencias bibliográficas

Bibliografía básica

- "User's Guide To Cryptography And Standards”

  Alex W. Dent, Chris J. Mitchell

  Artech House, 2004

- "Handbook of Applied Cryptography”

  Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone,

  CRC Press, 1996

Bibliografía complementaria

- *ISO 7498-2*
  - Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture, 1989.
- *RFC 2828*
  - RFC2828: Internet Security Glossary, R. Shirey, May 2000.
- *ITU-T X.800*
  - Recommendation X.800: Security Architecture for Open Systems Interconnection for CCITT Applications, ITU, 1991.
- *ITU-T X.509*
  - Recommendation X.509: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, ITU, 2005