Unidad 7:
EL FACTOR HUMANO EN LA CIBERSEGURIDAD

BLOQUE II – Sistemas, aplicaciones y personas

CONTENIDOS

1. Introducción.
2. Amenazas internas.
3. Ingeniería social.
4. Políticas y procedimientos.
5. Modelos de negocio.
6. Marco regulatorio.

1. Introducción

- El componente más débil para la seguridad de cualquier infraestructura TIC en la actualidad suele ser el factor humano.
  - Este factor suele implicar los mayores riesgos y amenazas.
- Como veremos, los atacantes maliciosos externos no siempre son la causa de los peores problemas de seguridad.
  - En muchos casos basta con usuario interno descuidado, poco concienciado o enfadado.

1. Introducción

La seguridad por oscuridad no funciona → Tampoco por prohibiciones ni legislación → Deben definirse políticas y procedimientos

2. Amenazas internas

- Con este término nos referimos al “enemigo en casa”.
- Es una de las amenazas que más preocupan en los últimos años, ya que suele ser difícil de prevenir, detectar, etc.
- Todos conocemos WikiLeaks o los casos de Snowden, Manning o Falciani.
  - Por mencionar sólo algunos ejemplos.
- Las motivaciones de una persona para convertirse en este tipo de amenaza pueden ser muy diversas.

2. Amenazas internas

- Este tipo de amenazas han llevado a las organizaciones a plantear ITPs (ITP = Insider Threat Program), que combinan:
  - Medidas técnicas: Herramientas que permiten clasificar los documentos por niveles de seguridad, control de accesos y autenticación con grano muy fino, sistemas de logs y auditoría detallados, etc.
  - Medidas organizativas: Definición clara de roles y responsabilidades, ubicación de equipos y monitores, uso de medios de almacenamiento extraíble o BYOD, etc.
  - Medidas de recursos humanos: Horarios, planes de concienciación, formación, incentivos, etc.

2. Amenazas internas

- Hay que ser cuidadosos, porque el control excesivo, la fiscalización constante y "el nivel de paranoia" de algunas organizaciones en este sentido ha terminado por ser contraproducente.

3. Ingeniería social

- La ingeniería social consiste en basarse en la buena/mala fe de las personas de una organización para obtener de ellas información valiosa que ayude a materializar una amenaza.
  - Para ello se utilizan técnicas psicológicas y habilidades sociales.
- Estas técnicas se llevan a cabo sobre:
  - Personal con falta de conciencia acerca del problema de seguridad informática.
  - Personal descontento.
- Y en muchos casos se aprovechan de una pobre concienciación.

3. Ingeniería social

- Técnicas pasivas:
  - Observación.
- Técnicas activas no presenciales:
  - Suplantando al administrador, al servicio de soporte, etc.:
    - Teléfono.
    - Mail.
    - Mensajería instantánea.
  - Baiting (USB malicioso o similar).

3. Ingeniería social

- Técnicas presenciales no agresivas/agresivas:
  - Buscando en la basura (dumpster diving).
  - Mediante seguimiento de personas y vehículos.
  - Vigilando salas y edificios.
  - Aprovechando situaciones de crisis.
  - Suplantación de personalidad.
  - Soborno, chantaje o extorsión.
  - Presión psicológica.

3. Ingeniería social

- El phishing es una técnica específica que consiste en jugar con la probabilidad.
  - Intentos masivos.
- El caso típico persigue extraer información confidencial (principalmente, el nombre de usuario y contraseña) enviando a todas las víctimas potenciales una comunicación confiable y legítima solicitándoles dicha información (por mail casi siempre).
  - Aparecen también los conceptos de Spear phishing (cuando el objetivo es un determinado grupo de personas, el ataque es dirigido) o Whaling (si el objetivo son los directivos de la organización).

3. Ingeniería social

- Otro caso habitual es el de la activación de un link vinculado a un correo electrónico en el que las víctimas confían y que implica la descarga de un software malicioso.
- Las contramedidas desplegadas por la organización deberían detectarlo e inutilizarlo.
  - Pero de nuevo se juega con la probabilidad.
  - Y con la información recogida con anterioridad.
    - Se puede explotar una vulnerabilidad que se haya descubierto previamente.

3. Ingeniería social

- Pregunta: ¿Qué es un watering hole, a qué nos referimos con este término en ciberseguridad?

3. Ingeniería social

- Pregunta: ¿Qué se puede hacer para reducir el impacto de estas técnicas sociales?

3. Ingeniería social

- Repuesta- Algunos ejemplos:
  - Implantar planes de concienciación y formación acerca de la importancia de la seguridad en el más amplio sentido de la palabra.
  - Limitar la información de público acceso, trabajar con mínimo privilegio, etc.
  - Utilizar mecanismos adecuados de autenticación y control de acceso.
  - Definir y mantener actualizadas políticas de seguridad adecuadas al entorno de operación de la organización (ahora lo vemos).

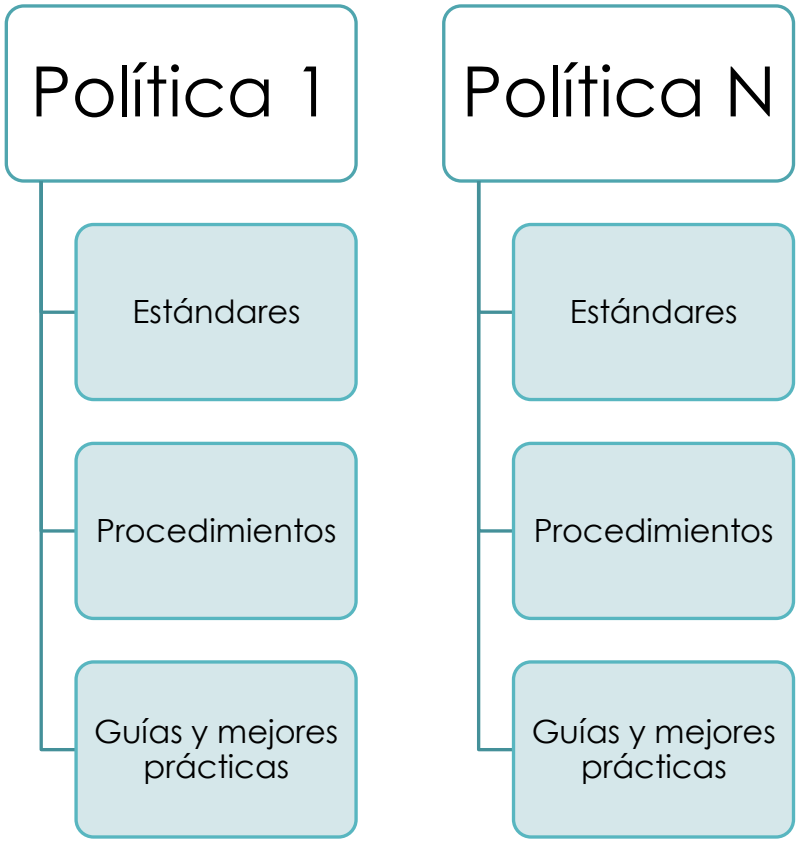
4. Políticas y procedimientos

- Las empresas y administraciones necesitan cada vez más un CSO (Chief Security Officer) o un CISO (Chief Information Security Officer).
- Una de las responsabilidades del departamento/área que depende directamente de esta persona suele ser definir un entorno de políticas y procedimientos que intenten gestionar el factor humano.
  - Gran importancia de la formación y concienciación dentro de los actuales Planes Directores de Seguridad.

4. Políticas y procedimientos

Bien documentadas

BIEN COMUNICADAS



4. Políticas y procedimientos

- **Título de la Política:** Enunciado corto y de fácil comprensión que proporciona una línea de acción desde la dirección.
- **Estándares**: Traducción de estas políticas a detalles concretos de uso de HW y SW para los usuarios.
- **Procedimientos**: Instrucciones concretas acerca de cómo cumplir las políticas teniendo en cuenta los estándares. Suelen definir planes de instalación, testeo, administración, configuración, etc. para administradores y otros responsables.
- **Guías y mejores prácticas:** Completan los estándares y procedimientos con sugerencias que no son de obligado cumplimiento pero que pueden el trabajo de administradores y usuarios, etc.

4. Políticas y procedimientos

- Ejemplos de políticas típicas:

Acceptable use policy (AUP)

- Define lo que la organización permite y no permite hacer a los empleados con los activos que le pertenecen (User Domain)

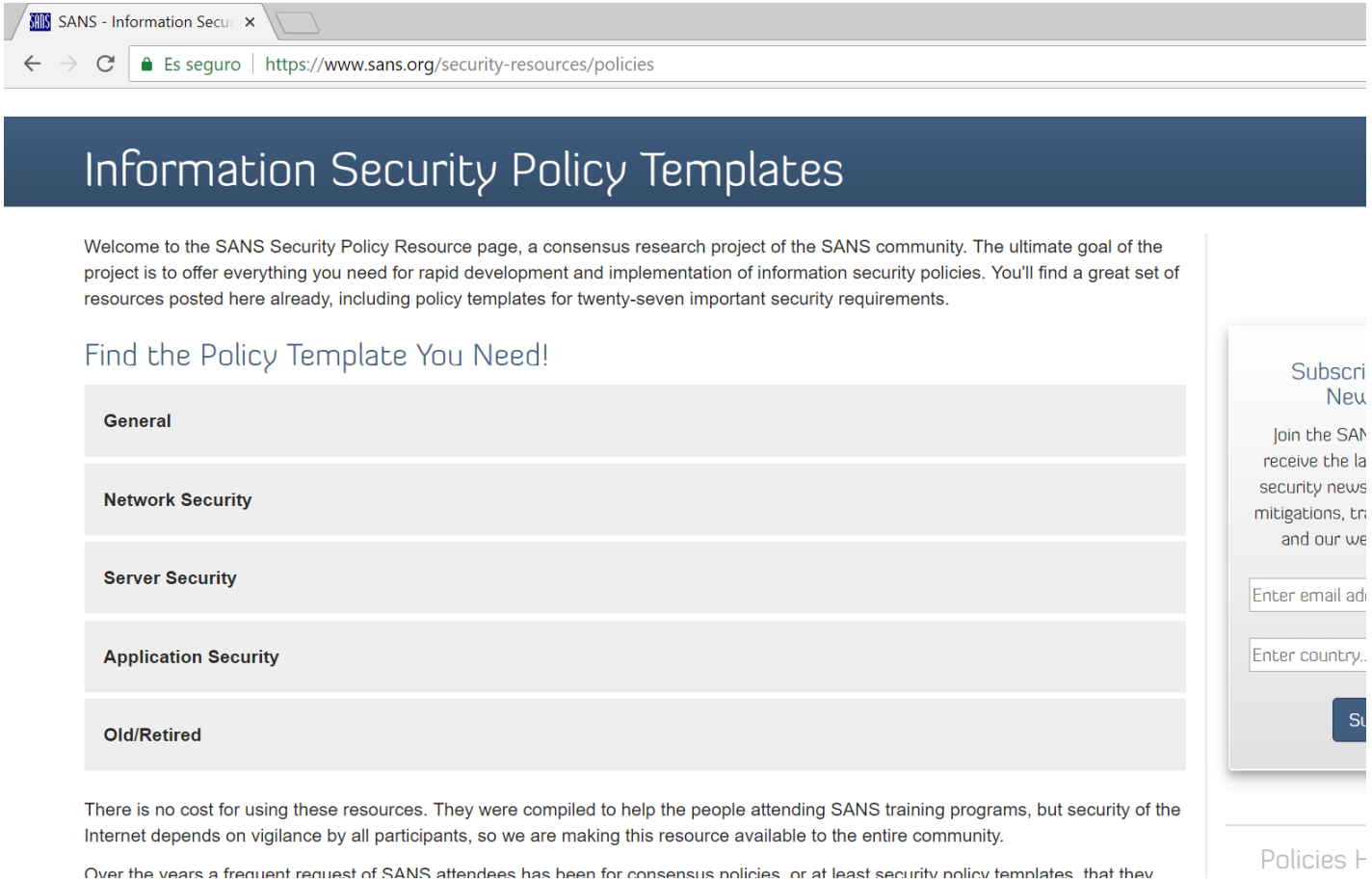
Security awareness policy

- Especifica cómo se asegura que el personal tiene la conciencia necesaria acerca de SI (User Domain)

Asset classification policy

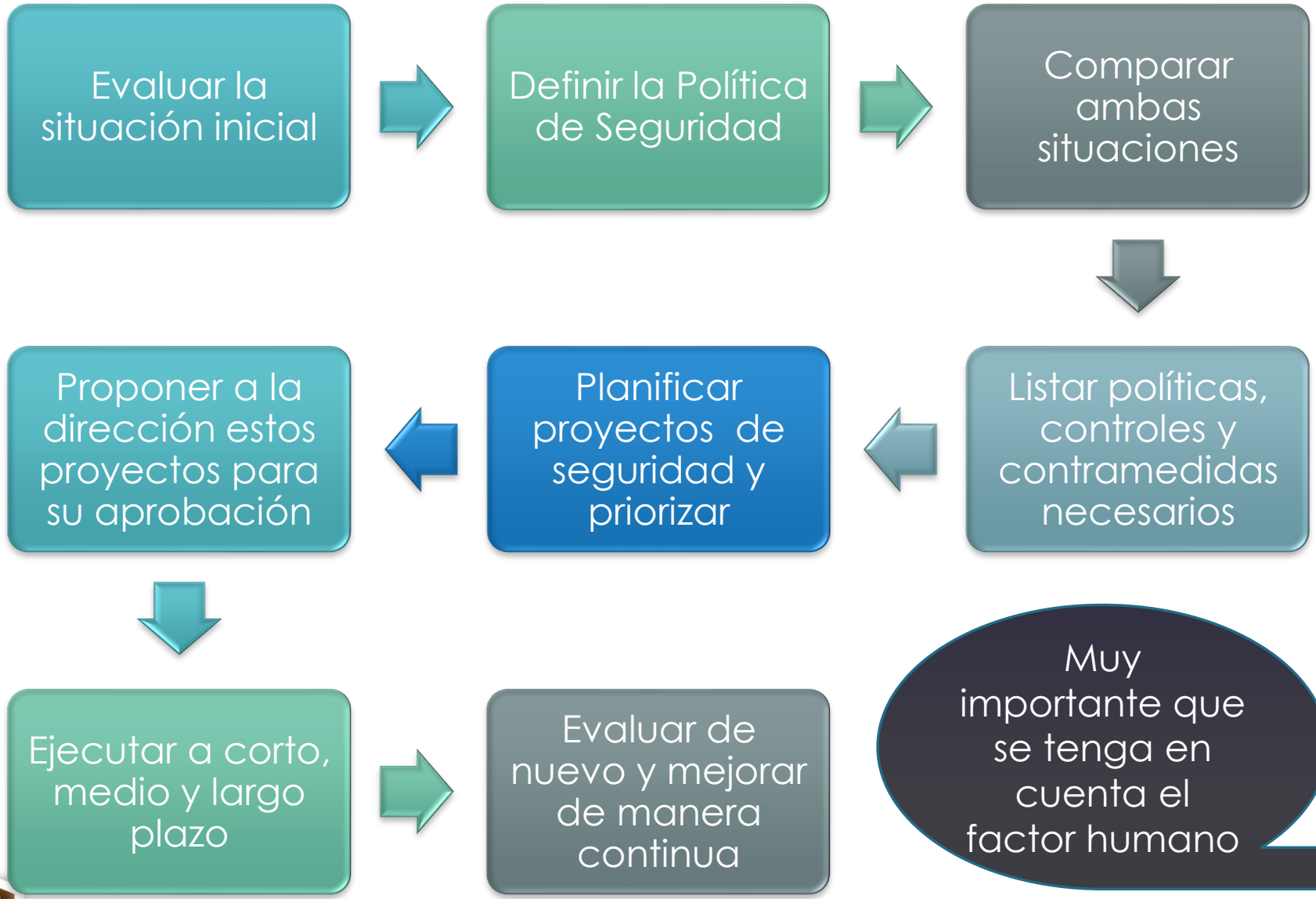
- Define cómo se realiza el inventario y clasificación de los activos de la organización en los siete dominios en función de su criticidad para el funcionamiento de la organización

4. Políticas y procedimientos



4. Políticas y procedimientos

- Un Plan Director de Seguridad consiste en “la definición y priorización de un conjunto de proyectos en materia de seguridad de la información dirigido a reducir los riesgos a los que está expuesta la organización hasta unos niveles aceptables”.
  - Es fundamental para la realización de un buen Plan Director de Seguridad que defina las obligaciones y buenas prácticas de seguridad que deberán cumplir los trabajadores de la organización así como terceros que colaboran con ésta, es decir, las políticas de seguridad.
  - Entre otros muchos factores.


Evaluar la situación inicial
Definir la Política de Seguridad
Comparar ambas situaciones
Listar políticas, controles y contramedidas necesarios
Planificar proyectos de seguridad y priorizar
Proponer a la dirección estos proyectos para su aprobación
Ejecutar a corto, medio y largo plazo
Evaluar de nuevo y mejorar de manera continua
Muy importante que se tenga en cuenta el factor humano

5. Modelos de negocio

- El cibercrimen es uno de los mercados mafiosos que más volumen de negocio mueve todos los años.
  - Comparable al tráfico de armas, de personas o de drogas.
- Por eso la necesidad de crear compañías que comercialicen productos/servicios dedicados a la prevención, detección y respuesta, de formar a las Fuerzas y Cuerpos de Seguridad del Estado y a los servicios de inteligencia.
- Y de tener profesionales capaces de dar respuesta a la demanda de trabajadores del sector.

5. Modelos de negocio

- Perfiles de cibercriminales

Intermediarios (IRC, Dark web)

Desarrolladores

Administradores de red

Diseñadores/arquitectos

Expertos en descubrimiento de vulnerabilidades, penetración e intrusiones

"Mulas"

Especialistas en criptomoneda

5. Modelos de negocio

Robo de números de tarjetas de crédito e info bancaria	Instalación de adware	Ransomware
Espionaje industrial	Venta de vulnerabilidades, malware o exploits	Spam o phising
Alquiler de botnets	Venta de info médica o genética	Criptojackers

- El cibercrimen como servicio ha supuesto un salto cuantitativo y cualitativo.

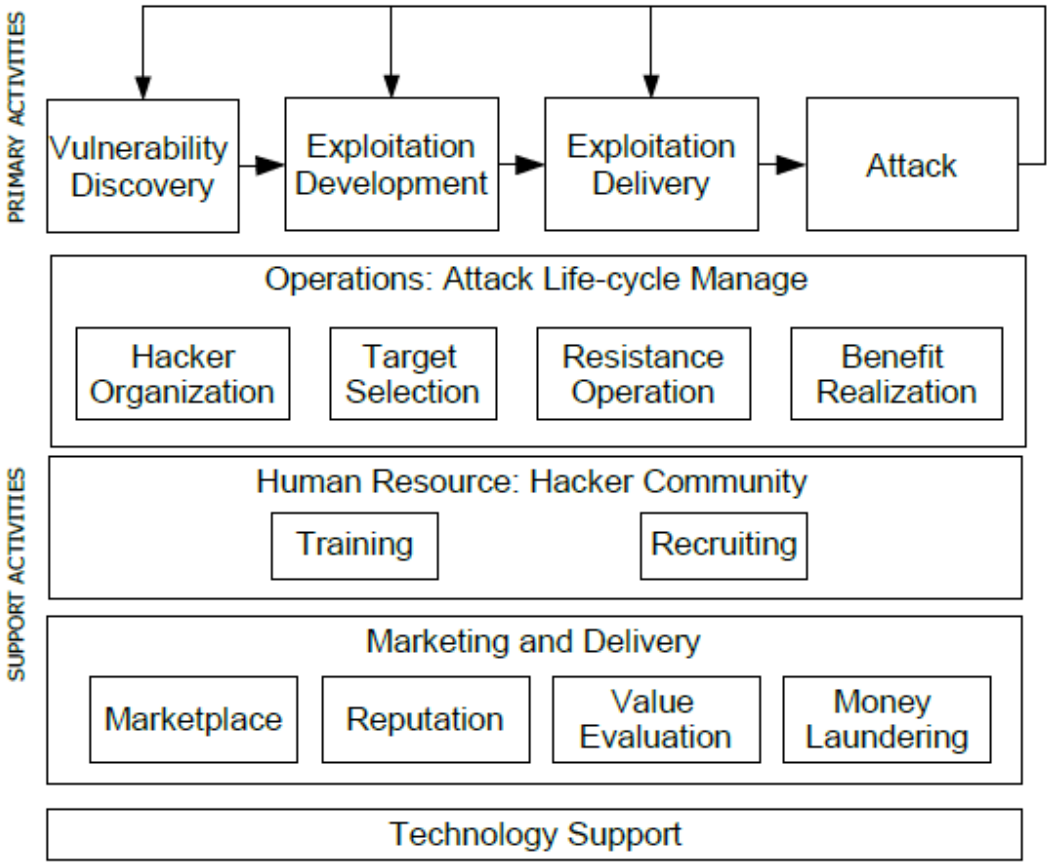


Fig. 1. Cybercriminal Value Chain Model

Cybercrime-as-a-Service: Identifying Control Points to Disrupt

KEMAN HUANG, MICHAEL SIEGEL, and STUART MADNICK, Massachusetts Institute of Technology, 2017

6. Marco regulatorio

- Un delito informático o ciberdelincuencia es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.
  - Delitos que tienen como objetivo equipos o redes de computadores, por ejemplo spam, propagación de malware o robo de información.
  - Delitos realizados por medio de ordenadores y de Internet, por ejemplo, espionaje, fraude y robo, acoso o pornografía infantil.

6. Marco regulatorio

- En Europa se regulan a través del convenio sobre la ciberdelincuencia (2001) que establece un marco común en el que:
  - Constituyen un delito informático todos aquellos delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos.
- Aunque cada vez existen más problemas con la determinación de la jurisdicción competente.
  - Cloud, móviles, redes sociales.

6. Marco regulatorio

Legislación española sobre seguridad informática y ciberdelincuencia

- Código penal.
- Ley de servicios de la sociedad de la información.
- Ley orgánica de protección de datos personales y garantía de los derechos digitales.
- Leyes de propiedad intelectual, firma electrónica, comunicaciones, etc.

Esquema Nacional de Seguridad

Ley de Protección de Infraestructuras Críticas

Ley NIS

6. Marco regulatorio

- **Delitos recogidos en el Código Penal (I):**
  - Descubrimiento y revelación de secretos (incluye hacking ético): Artículo 197 C.P.
  - Espionaje informático empresarial: Artículo 278 C.P.
  - Daños informáticos o sabotaje (incluye hacktivismo): Artículo 264.2 C.P.
  - Pornografía infantil: Artículo 189 C.P.
  - Calumnia: Artículos 205 y 206 C.P
  - Injuria: Artículo 208 y 209 C.P.
  - Calumnias e injurias hechas con publicidad: Artículo 211 C.P.
  - Delito tradicional de daños: Artículo 263 C.P

6. Marco regulatorio

- **Delitos recogidos en el Código Penal (II):**
  - Hurto: Artículo 234 C.P
  - Robo: Artículo 237 C.P.
  - Defraudaciones de fluido eléctrico: Artículo 255 C.P.
  - Defraudación a través de equipo terminal de comunicaciones: Artículo 256 C.P
  - Delitos contra la propiedad intelectual: Artículos 270 y 271 C.P
  - Delitos contra la propiedad industrial: Artículo 273 C.P.
  - Publicidad ilícita: Artículo 282 C.P.
  - Falsedad de documento público: Artículo 390 C.P.
  - Falsedad de documento privado: Artículo 395 C.P.
  - Difusión de protestas: Artículo 559 C.P.

6. Marco regulatorio

- La Ley de Servicios de la Sociedad de la Información (LSSI) se aplica a los siguientes servicios de la Sociedad de la Información, cuando constituyan una actividad económica o lucrativa para el prestador:
  - Comercio electrónico.
  - Contratación en línea.
  - Información y publicidad.
  - Servicios de intermediación.
- Se refiere a la calidad del servicio, plazos, formas de contratación y pago, cookies, etc.

6. Marco regulatorio

- Además esta ley se basa en un límite para la tenencia y utilización de datos personales así como sobre el tráfico de los mismos.
  - Lo establece la Ley Orgánica de Protección de Datos (LOPD) que está de plena actualidad por la entrada en vigor del GDPR europeo.
  - La Agencia Española de Protección de Datos se encarga de facilitar al ciudadano el derecho a conocer quién está utilizando sus datos personales y para qué, y negar el permiso sobre el uso de sus datos a quien considere oportuno, etc.

6. Marco regulatorio

- En cuanto a la ley de la propiedad intelectual es el conjunto de normas conducentes a la protección de la creación, mediante el reconocimiento de una serie de derechos a favor de los autores y de los otros titulares.
  - La propiedad intelectual es privada, y se presta la obra protegida bajo esta propiedad según le venga en gana al propietario y/o al creador, para fines principalmente económicos.
  - Esta ley también se encuentra en constante debate en la actualidad.

6. Marco regulatorio

- **Delitos más comunes contra la propiedad intelectual:**
  - Robo de contenidos de páginas web y blogs.
  - Robo de dominios.
  - Copias ilegales de música, películas, libros, software, etc.
  - Creación, distribución o tenencia de *cracks* que permiten saltarse los sistemas de protección de la propiedad intelectual.
  - Comercio a través de Internet de productos patentados sin autorización del titular de la patente.

6. Marco regulatorio

Asignaturas completas: **Dimensiones y modelo de la seguridad**, este mismo curso pero en el segundo cuatrimestre, y **Principios Jurídicos Básicos aplicados a la Ciberseguridad** el próximo curso

Para practicar un poco

1. Busca algún ejemplo reciente que haya trascendido de una compañía que haya sufrido una amenaza interna e investiga acerca de sus consecuencias e impactos, de la motivación de la persona involucrada, etc.
2. Diseña (pero no pongas en práctica) un ataque de whaling. Detalla el objetivo del atacante, los medios empleados (cómo es el email que se envía, por ejemplo), la planificación, etc. Y explora qué tipo de herramientas adicionales podrías emplear para aumentar tus posibilidades de éxito.

Referencias

- Fotografías
  - https://unsplash.com
- Iconos
  - https://www.flaticon.es/

Reconocimiento-CompartirIgual 3.0 España (CC BY-SA 3.0 ES)