Integración de Seguridad Informática en Redes y Sistemas de Software
TC2007B

M2: Seguridad en aplicaciones y redes

Profesor de Cátedra:

Osvaldo Cecilia Martínez

osvaldo.cecilia@tec.mx

Semana 2

2.2. Requisitos de seguridad y diseño

I. SDL

II. Análisis de riesgos

III. Identificar estándares y normas

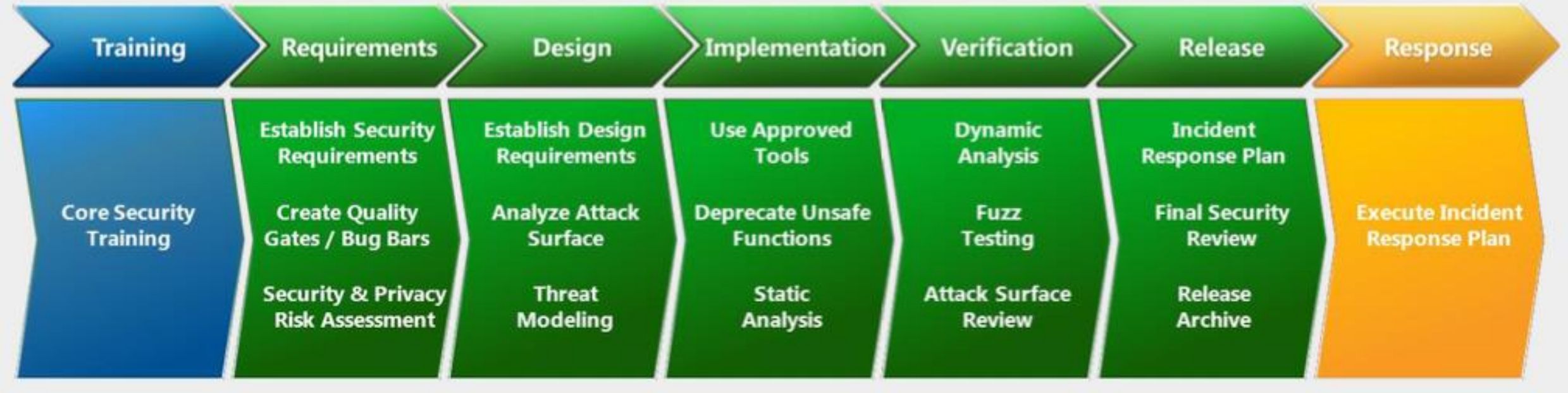
IV. Definir requisitos de seguridad

V. Establecer niveles mínimos de seguridad

Reflexión:
¿Cómo podemos defendernos de las amenazas si no las conocemos?

2.2 Requisitos de seguridad y diseño

Security Development Lifecycle (SDL)



Fuente: https://www.microsoft.com/en-us/securityengineering/sdl/

Security Development Lifecycle (SDL)

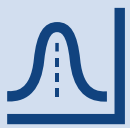
1. Establecer estándares de seguridad, métricas y gobernanza
2. Uso de elementos de seguridad aprobados, lenguajes y frameworks
3. Revisión de diseño de seguridad y modelado de amenazas
4. Definir y utilizar estándares de criptografía
5. Asegure la cadena de suministro de software
6. Asegure el entorno de ingeniería
7. Realizar pruebas de seguridad
8. Garantizar la seguridad de la plataforma operativa
9. Implementar monitoreo de seguridad y respuesta
10. Proporcionar entrenamiento de seguridad

Fuente: https://www.microsoft.com/en-us/securityengineering/sdl/practices

Análisis de Riesgos (primera aproximación)

Detectar activos y configuraciones

Identificar vulnerabilidades y amenazas



Estimar la probabilidad e impacto

Estimar y evaluar el riesgo

Análisis de Riesgos: Activos

Detectar activos y configuraciones

Los sistemas de información son conjuntos de componentes y sus relaciones, los cuales, nos permiten ejecutar procesos de negocio.

Proceso clave: adecuada gestión de activos y configuraciones.

Análisis de Riesgos: Activos

Detectar activos y configuraciones

Ejemplos:

- Aplicaciones (web app, mobile app, web service)
- Frameworks de desarrollo (React, Angular)
- Bibliotecas de software (SoundJS, SwiperJS)
- Gestores de bases de datos (MS SQL, Mongo)
- Sistemas operativos (Windows, Unix)
- Redes de comunicaciones (protocolos, puertos)

Análisis de Riesgos: Vulnerabilidades

Identificar vulnerabilidades y amenazas

Presentes en:

- Diseño
- Desarrollo
- Configuración
- Liberación
- Operación

Análisis de Riesgos: Vulnerabilidades

Identificar vulnerabilidades y amenazas

Fuentes de información:

- Escaneo de vulnerabilidades
- Bases de datos de vulnerabilidades
- Fabricantes
- Fuentes especializadas

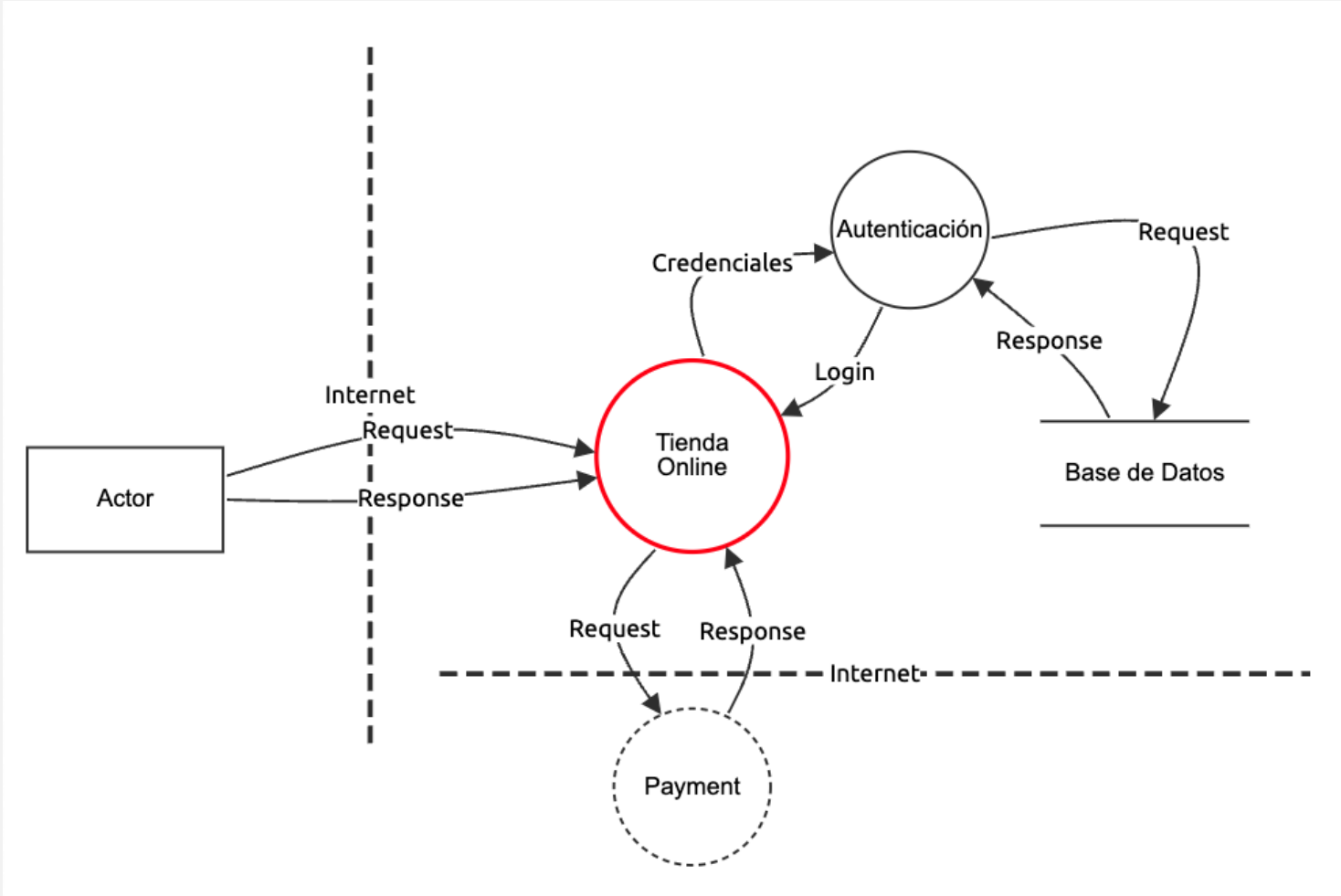
Análisis de Riesgos: Modelado de Amenazas

1. Definición de activos y sus interacciones

2. Diagrama: procesos, actores, almacenamiento y flujo de datos

3. Por cada elemento se identifican las diferentes amenazas

Análisis de Riesgos: Modelado de Amenazas



Análisis de Riesgos: Modelado de Amenazas

Modelo STRIDE

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of priviledge

Definición	Ejemplo
Hacerse pasar por algo o por otra persona	Robo de credenciales de un usuario legítimo
Modificación de datos o código	Alteración de un paquete que viaja por una LAN
Afirmar no haber realizado una acción	"Yo no envié ese correo electrónico"
Exponer información a alguien no autorizado a verla	Publicar una lista de clientes con datos sensibles en un sitio web
Denegar o degradar el servicio a los usuarios	Sobrecarga los servidores de un sitio web
Obtener capacidades sin la debida autorización	Explotar una vulnerabilidad para obtener permisos de administrador en un sistema

Análisis de Riesgos: Modelado de Amenazas

Otros modelos comienzan por definir todos los tipos de actores , sus capacidades y qué impactos pueden tener sobre los activos.

Activo	C	I	A
Web Server	Intrusión	Ransomware Defacement	DDoS
DB	Robo de datos personales	Ransomware	Bloqueo
Reputación	Robo de información de clientes		

Análisis de Riesgos: Modelado de Amenazas

Herramientas:

Microsoft Threat Modeling Tool

OWASP Threat Dragon

Análisis de Riesgos: Impacto y Probabilidad

Tipos de Valores

Cuantitativo: valor numérico que indica la probabilidad o impacto.

La probabilidad podría estar entre 0 o 1, o indicar cuántos eventos esperamos en un período. Para el impacto, podrían ser días sin servicio, cantidad de datos expuestos o dinero incluido.

Puede resultar difícil estimar con precisión.

Cualitativo: Descripciones como alto, bajo o medio.

Si bien es más fácil de determinar, es posible que no refleje la probabilidad o el impacto reales.

Es subjetivo

Análisis de Riesgos: Impacto y Probabilidad

Impacto: depende de los factores que decida la organización. Por ejemplo:

- **Alto**: no es posible continuar con la operación
- **Medio**: prevalece un funcionamiento degradado
- **Baja**: la operación puede continuar, pero con algunos problemas

Probabilidad: Depende de lo fácil que sea para un atacante materializar el riesgo.

- **Alto**: Muy fácil, puede ocurrir en cualquier momento
- **Medio**: Podría ocurrir con conocimiento especializado
- **Baja**: Muy difícil de materializar, no ocurre normalmente.

Análisis de Riesgos: Matriz de Riesgos

		Impacto		
		Alto	Medio	Bajo
Probabilidad	Alto	Alto	Alto	Medio
	Medio	Alto	Medio	Medio bajo
	Bajo	Alto/medio	Bajo	Bajo

Alto: acción correctiva obligatoria

Medio: acción correctiva sugerida

Bajo: Acción correctiva deseada pero no necesaria/Supervisión o monitoreo

Análisis de Riesgos: Caso

Supranet is a startup that offers a product for network administration. It has 5 employees. 1 is the owner, 3 are programmers/IT, and the last one does sales and marketing. In their office they have a 2 production servers, one for the web application, and another for the database. They also have one server for testing that replicates their webserver and has a small database, and another a last one with CRM software to handle their 134 clients data.

They have a 500 Mbps DSL connection, and a laptop for each employee, all with antivirus and firewall. Also, all the servers and computers have a backup in the cloud using AWS Glacier. The backup is done weekly.

Each client pays a 3,000 pesos fee to use the platform and can register up to 500 network devices. Clients can make requests where they upload a pdf to the page and the programmers decide if they implement it. Last week, via this submission a programmer opened an infected pdf which contained a ransomware and they lost a week of work from their computer.

Análisis de Riesgos: Actividad – Parte 1

1. A partir del escenario, determina las interacciones utilizadas con el modelado de amenazas (CIA, STRIDE)
2. Selecciona 3 activos y completa la tabla de riesgos CIA con 9 riesgos
3. Para los riesgos identificados:
    a. Estima el impacto y la probabilidad
    b. Estima el nivel de riesgo.

*No enviar todavía. Espera la 2ª parte.

¿Tienes alguna duda?