



Universidad Nacional
Federico Villarreal



INGENIERIA DE SISTEMAS DE INFORMACIÓN

Docente: Ing. Alejandro Rea
Lima Perú Julio 2025
Sesión 13



¿En qué
consiste la
Identificación
y Formulación
del
Problema?



Es la **primera etapa del ciclo de vida del desarrollo de software**, donde se define claramente **qué problema se quiere resolver, a quién afecta y qué alcance tendrá la solución**. Es el fundamento para evitar errores costosos en etapas posteriores.

Objetivos principales:

- Comprender el contexto y la necesidad del cliente o usuario.
- Delimitar el problema real (no solo los síntomas).
- Establecer metas claras para el sistema.
- Documentar requerimientos iniciales (funcionales y no funcionales).
- Justificar la necesidad de una solución tecnológica.

Metodologías para la Identificación y Formulación del Problema

1. Design Thinking:

- Centrado en el usuario.
- En la fase de Empatizar e Identificar el problema, se recolecta información mediante entrevistas, encuestas, observación directa, etc.
- El How Might We...? ayuda a formular el problema en forma de oportunidad.

2. Soft Systems Methodology (SSM):

- Muy útil en sistemas complejos, sociales y con múltiples partes interesadas.
- Usa diagramas de causa-efecto, CATWOE (Cliente, Actor, Transformación, Weltanschauung, Owner, Environment) para formular problemas.

3. Análisis de Problemas (Problem Analysis):

- Parte del Business Analysis Body of Knowledge (BABOK).
- Identifica causas raíz (por ejemplo, usando Ishikawa o 5 Why's).
- Define claramente las brechas entre el estado actual y el deseado.

4. UML – en esta fase se usan:

- Casos de uso preliminares
- Modelos de contexto
- Para representar actores y procesos que participan en el sistema actual o deseado.

5. Lean Startup o MVP (Minimum Viable Product):

- En entornos ágiles, se plantea una hipótesis de problema y se valida rápidamente con un prototipo funcional.

Caso Práctico:

Sistema de Gestión de
Citas Médicas para un
Centro de Salud



Contexto:

El centro de salud "Salud Integral" atiende a más de 200 pacientes diarios, pero usa agendas físicas para programar citas. Se producen errores como duplicación, pérdida de citas o tiempos de espera prolongados.



Identificación del Problema:

- **Problema central:** Ineficiencia en la gestión manual de citas médicas.

- **Causas:**

- Agenda física propensa a errores humanos.
- Falta de control de disponibilidad de médicos.
- Los pacientes deben acudir presencialmente o llamar para obtener una cita.

Identificación del Problema:

- **Consecuencias:**

- Pacientes insatisfechos.
- Médicos con tiempos mal distribuidos.
- Pérdida de ingresos por citas no asistidas o mal gestionadas.

Metodología Aplicada: Design Thinking

- Se realizaron entrevistas a personal administrativo, médicos y pacientes.
- Se identificaron puntos de dolor en el proceso actual.
- Se formuló el problema:
“¿Cómo podríamos mejorar la programación de citas para que pacientes y médicos tengan una experiencia más eficiente y organizada?”

Formulación del problema:

"El centro de salud Salud Integral enfrenta dificultades en la gestión de citas debido a la utilización de métodos manuales.

Formulación del problema:

Esto genera pérdida de tiempo, sobrecarga administrativa y molestias a los pacientes.

Formulación del problema:

Se requiere el desarrollo de un sistema de gestión digital de citas que automatice la programación, control de disponibilidad y envío de recordatorios."

Resultado Esperado:

Sistema Web/Móvil de gestión de citas, con calendario, gestión de disponibilidad médica, notificaciones automáticas, historial de citas, y panel administrativo.

Conclusión:

La identificación y formulación del problema es clave para que un proyecto de software tenga éxito. Si no se define bien el problema, se corre el riesgo de construir una solución que no sirva.

Conclusión:

Aplicar metodologías adecuadas garantiza una comprensión profunda del contexto y permite construir soluciones tecnológicas alineadas a necesidades reales.

“Hackers” ya no necesitan vulnerar sistemas de seguridad: Ahora apuntan a trabajadores de bancos

Los cibercriminales no requieren romper barreras tecnológicas: en Latinoamérica el 80% de los casos de cibercrímenes incluía el factor humano y persuadir a personas para acceder a datos sin soltar alarmas



En Perú desde el año pasado han resonado más los casos de **cibercrimenes**, aquellos que no solo involucran fraude digital, estafas con inteligencia artificial y otras modalidades para robar dinero de ciudadanos, sino también el filtrado de datos sensibles de clientes de bancos y entidades similares (Véase el [caso de Interbank](#), el de [Inkafarma](#), el evento reciente de supuesto filtrado de información del [Banco de la Nación, etc.](#)).

Si bien algunas entidades no afirma ni niegan que se haya dado este filtrado de datos, y comunica más que no se ha vulnerado la seguridad digital de sus sistemas (esto supone la ruptura de una barrera tecnológica, un “**hackeo**”, un acceso no autorizado) o que los datos no suponen acceso directos a cuentas en bancos, un informe de Marsh McLennan sugiere que los *cibercriminales* no dejan este rastro y no sueltan alarmas digitales.

“En los últimos años, las pérdidas por ciberataques basados en el sector retail se han incrementado significativamente a nivel global, principalmente a través del engaño a las personas, es decir, ataques de ingeniería social. Esta modalidad **no requiere malware sofisticado**, ni brechas técnicas, basta con una llamada falsa al área de soporte o un correo que aparenta ser de un superior para abrir la puerta a la violación del sistema”, afirma el la empresa líder global en riesgo, estrategia y personas.




Filtración de datos de Interbank por supuesto 'hacker' habría puesto en peligro datos de alrededor de tres millones de clientes. - Crédito Composición Infobae/Interbank/Andina

Ciberataques a los trabajadores

Ocho de cada diez ciberataques apuntan al factor humano, señala el informe de Marsh McLennan. “Esta forma de operar es cada vez más común en América Latina y ha ayudado a comprometer a grandes compañías de múltiples sectores, aprovechando el error humano con una precisión alarmante”

Perú no es la excepción. Si bien en el país también tiene que lidiar con la extorsión y trabajadores de bancos que pueden estar coludidos con delincuentes, también en el país se reportan filtrados de datos que, en varias ocasiones no nacen de una vulneración de sistemas de seguridad de las entidades.

“Esta técnica ha sido perfeccionada por grupos cibercriminales altamente sofisticados como **Scattered Spider**, cuyo accionar ha afectado a importantes empresas del sector retail en Estados Unidos y el Reino Unido. Lo que hace especialmente peligroso a este grupo es su combinación de habilidades técnicas avanzadas, con un alto dominio de la manipulación psicológica”, explica Marsh McLennan.

| | | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|-----------------------|-------------------|
|  Centro Nacional de Seguridad Digital | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 032 | | Fecha: 07-02-2025 |
| | | | Página: 6 de 7 |
| Componente que reporta | CENTRO NACIONAL DE SEGURIDAD DIGITAL | | |
| Nombre de la alerta | Supuesta base de datos de clientes de Inkafarma está a la venta | | |
| Tipo de Ataque | Fuga de Información | Abreviatura | FugaInfo |
| Medios de propagación | Red, Internet, Redes sociales | | |
| Código de familia | K | Código de Sub familia | K02 |
| Clasificación temática familia | Uso inapropiado de recursos | | |
| Descripción | | | |
| 1. ANTECEDENTES: | | | |
| Se publica posible compromiso de Base de datos estructurada con detalles personales de clientes de Inkafarma. | | | |
| 2. DETALLES: | | | |
| Se detectó una publicación en un foro de hackers en la que un actor de amenazas afirma que la empresa farmacéutica Inkafarma ha sufrido una vulneración de seguridad y los registros de sus clientes ahora están en la Dark Web. | | | |
| De hecho, indican estar vendiendo la supuesta base de datos de los clientes. | | | |
| Según el actor de amenazas conocido como @IntelBrokerBF, la vulneración ocurrió el 6 de febrero de 2025 y afecta aproximadamente a 3,9 millones de registros. El conjunto de datos incluye información confidencial de los clientes, como números de identificación (DNI), números de teléfono, direcciones de correo electrónico, nombres, fechas de nacimiento y otros detalles personales. | | | |

Así se vió el reporte del Centro Nacional de Seguridad Digital que fue emitido por el caso del 'hackeo' a Inkafarma. - Crédito Captura del Centro Nacional de Seguridad Digital

Si bien se habla del caso extranjero, este sería el modelo para los cibercriminales en Latinoamérica, que operarían con técnicas dirigidas a persuadir a trabajadores y colaboradores de las mismas empresas, para tener acceso a datos internos sin necesidad de *vulnerar una barrera tecnológica*.

“Scattered Spider ha demostrado una capacidad inusual para suplantar identidades en llamadas a servicios de soporte, accediendo a sistemas críticos **sin levantar sospechas, ni activar alertas automáticas**. Sus ataques han generado interrupciones operativas prolongadas, pérdidas económicas millonarias y caídas significativas en el valor de las acciones de empresas afectadas, evidenciando su alto nivel de impacto”, añade.

Es así que lo que preocupa es que “ya no se trata de un grupo aislado, sino de diversas *bandas criminales* en el mundo están adoptando este enfoque, elevando el nivel de exposición para las empresas en América Latina”.



El Banco de la Nación no desmintió que se estén poniendo en venta datos de clientes en foros de "hackers", pero sí dijo que en sus sistemas no hubo vulneración. Sin embargo, un informe revela que hay otra ruta en que se pueden obtener estos datos y sin soltar alarmas. - Crédito Banco de la Nación