Portafolio

Sala de los espejos: Experiencias de Aprendizajes

Taller de Comunicación (TCOM)

2º Cuatrimestre 2025

DOCENTES:

Denise Ramirez del Rio

Cinthia Cossio

Lucia Kazah

Equipo de trabajo - Comisión D

- Eduardo Moreno

Índice

Instituto de Formación Técnica Superior N.º 29

IFTS N.º 29

Tecnicatura Superior en Desarrollo de Software

Sala 4

Registro de la 1.ª actividad seleccionada:

Número y nombre de la sala:	Sala 4 “Requerimientos decodificados”
¿Es de Cámara o de Acción?:	Cámara
Nombre de la actividad:	Analizar para relevar

¿Por qué crees que esta actividad es obligatoria para la elaboración del portafolio?

Porque la elaboración de un requerimiento es esencial para establecer una comunicación clara y precisa entre las partes involucradas, garantizando que las necesidades queden bien definidas. Además, sirve como guía para orientar el desarrollo, evitando malentendidos y asegurando que el producto final cumpla con los objetivos planteados.

Caso 1

Dra. Rodríguez
CONTEXTO COMUNICATIVO 1
La Dra. Marta Rodríguez, cardióloga de la Clínica Médica “SUD”, comparte su día a día interactuando con él
sistema de historias clínicas.

"Cada vez que intento acceder a los historiales clínicos, me encuentro con problemas de autenticación. Las contraseñas actuales no ofrecen la seguridad necesaria para manejar la información delicada que manejamos en cardiología. La sensación de vulnerabilidad
persistente es frustrante, especialmente cuando la atención a los pacientes requiere rapidez y precisión."

"En mi especialidad, cada segundo cuenta, y la lentitud o inseguridad en el acceso a los historiales clínicos puede tener consecuencias críticas. La necesidad de una experiencia más fluida y segura es evidente, y lidiar con estos problemas de autenticación se ha convertido en una realidad frustrante en mi práctica diaria."

REQUERIMIENTO

“La nueva versión debe implementar un sistema de autenticación robusto, exigiendo contraseñas complejas y considerando la posibilidad de incorporar autenticación de dos factores para garantizar un acceso seguro.”

Cotejo

Lista de cotejo para revisar el requerimiento del sistema de autenticación

Empleá la lista de cotejo para distinguir entre lo que proporciona información ("Sí") y lo que está ausente ("No") del siguiente requerimiento:

"La nueva versión debe implementar un sistema de autenticación robusto, exigiendo contraseñas complejas y considerando la posibilidad de incorporar autenticación de dos factores para garantizar un acceso seguro".

✓ El requisito de exigir "contraseñas complejas" como parte del sistema de autenticación. *

- (●) Sí ✓
- ( ) No

✓ Detalles sobre cómo se garantizará la seguridad y confidencialidad de las contraseñas almacenadas: *

- ( ) Sí
- (●) No ✓

✓ Información sobre cómo se evaluará y gestionará la incorporación de autenticación de dos factores: *

- ○ Sí
- ◉ No ✓

✓ La consideración de la "posibilidad de incorporar autenticación de dos factores" para garantizar un acceso seguro. *

- ◉ Sí ✓
- ○ No

✓ La necesidad de implementar un "sistema de autenticación robusto" en la nueva versión del sistema de la historia clínica. *

- ◉ Sí ✓
- ○ No

✓ Roles y responsabilidades específicos en relación con la gestión y mantenimiento del sistema de autenticación: *

- ○ Sí
- ◉ No ✓

Requerimiento reformulado

"El nuevo sistema de seguridad, deberá tener una doble autentificación,

contraseña más robusta en seguridad, una vez ingresado, validaciones con token de seguridad.
- Doble autentificación:
El sistema debe requerir dos factores de autenticación para todo acceso al sistema:

1. Conocimiento: Contraseña personal del usuario.
2. Posesión: Token de seguridad generado por:
    - Aplicación autenticadora (Google Authenticator), o
    - Clave de seguridad física, o
    - SMS.

- El segundo factor debe ser obligatorio en cada inicio de sesión.
- El sistema debe permitir la recuperación segura del acceso en caso de pérdida del segundo factor, mediante un proceso validado por el administrador de seguridad.

- Contraseña robusta:
Las contraseñas deben cumplir con los siguientes requisitos mínimos:

- ☐ Mínimo 12 caracteres.
- ☐ Combinación de:
    - ☐ Letras mayúsculas (A-Z)
    - ☐ Letras minúsculas (a-z)
    - ☐ Números (0-9)
    - ☐ Caracteres especiales (!@#$%^&*)
- ☐ No reutilización de las últimas 3 contraseñas.
- ☐ Caducidad cada 90 días, con alertas de recordatorio.
- ☐ Las contraseñas deben almacenarse en la base de datos con hash criptográfico seguro (bcrypt).
- ☐ El sistema debe bloquear temporalmente la cuenta tras 5 intentos fallidos de inicio de sesión, con notificación al usuario y al administrador.

- Validación por Token:
Una vez autenticado, el sistema debe generar un token de sesión seguro (JWT) que:

- ☐ Tenga una duración máxima de 60 minutos de inactividad.
- ☐ Se invalide automáticamente al cerrar sesión o expirar.
- ☐ Incluya información cifrada del usuario, rol y tiempo de emisión.
- ☐ Sea transmitido mediante HTTPS/TLS para evitar interceptación.
- ☐ Los tokens deben ser almacenados de forma segura en el cliente (HttpOnly o cookies), nunca en localStorage.
- ☐ El sistema debe permitir la invalidación manual de sesiones activas desde el perfil del usuario o por el administrador.

“

Caso 2

Dra. Gómez
CONTEXTO COMUNICATIVO 2
La Dra. Ana Gómez, pediatra en la ClínicaMédica “SUD”, comparte las complicaciones que enfrenta con el sistema de permisos en las historias clínicas.

""Cada vez que reviso el sistema de historias clínicas, me encuentro con una neblina de incertidumbre. No sé quién más está ingresando, cuándo lo hacen o qué están haciendo. Es como trabajar en un área con ventanas opacas: me gustaría saber quién más está cuidando a mis pequeños pacientes y cómo se están manejando sus historiales médicos."
"La colaboración es esencial en pediatría, pero el sistema actual parece ocultar las interacciones entre médicos. No hay claridad sobre quién hizo qué y cuándo. Sería beneficioso para todos si pudiéramos entender mejor cómo se están gestionando los datos de nuestros pacientes, promoviendo una atención más integral y coordinada."

REQUERIMIENTO

“Con el objetivo de fortalecer la trazabilidad y garantizar la seguridad en la manipulación de la información, la nueva versión del sistema de permisos deberá incorporar un registro detallado. Este registro incluirá de manera explícita quién accede al sistema, los momentos precisos en que se realiza el acceso y las acciones ejecutadas por cada usuario. Esta implementación contribuirá significativamente a la transparencia y control de las operaciones en el sistema, brindando mayor confianza en la gestión de la información clínica.“

Cotejo

Lista de cotejo para revisar el requerimiento del sistema de permisos

Empleá la lista de cotejo para distinguir entre lo que proporciona información ("Sí") y lo que está ausente ("No") del siguiente requerimiento:

Con el objetivo de fortalecer la trazabilidad y garantizar la seguridad en la manipulación de la información, la nueva versión del sistema de permisos deberá incorporar un registro detallado. Este registro incluirá de manera explícita quién accede al sistema, los momentos precisos en que se realiza el acceso y las acciones ejecutadas por cada usuario. Esta implementación contribuirá significativamente a la transparencia y control de las operaciones en el sistema, brindando mayor confianza en la gestión de la información clínica."

✓ Información sobre la frecuencia con la que se realizará la revisión y análisis del registro detallado: *

- ○ Sí
- ◉ No ✓

✓ La indicación de que el registro detallado deberá registrar "en qué momentos" se accede al sistema. *

- ◉ Sí ✓
- ○ No

El énfasis en que la implementación brindará "mayor confianza en la gestión de la información clínica". *

- [x] Sí
- [ ] No

Detalles técnicos específicos de cómo se implementará el registro detallado: *

- [ ] Sí
- [x] No

Detalles sobre cómo se asegurará la integridad y confidencialidad del registro detallado: *

- [ ] Sí
- [x] No

El requisito de que el registro detallado debe registrar "qué acciones realiza" cada usuario. *

- [x] Sí
- [ ] No

✓ Roles y responsabilidades específicos en relación con la gestión y revisión del registro detallado: *

- ○ Sí
- ◉ No ✓

✓ Especificación clara de las acciones específicas que serán registradas en el sistema: *

- ○ Sí
- ◉ No ✓

✓ La necesidad de implementar un "registro detallado" en la nueva versión del sistema de permisos. *

- ◉ Sí ✓
- ○ No

✓ La especificación de que el registro detallado deberá indicar "quién accede al sistema". *

- ◉ Sí ✓
- ○ No

Requerimiento reformulado

“El sistema de permisos deberá incorporar un registro detallado que fortalezca la trazabilidad y garantice la seguridad en la manipulación de la información clínica. Este registro deberá incluir quién accede al sistema, en qué momentos lo hace y qué acciones realiza cada usuario. La implementación contribuirá a la transparencia, el control de las operaciones y la confianza en la gestión de la información clínica.”

Registro detallado:

- ☐ Se debe implementar un log de auditoría en la base de datos del sistema.
- ☐ El registro incluirá:
  - ☐ Usuario autenticado (ID único).
  - ☐ Fecha y hora exacta de inicio/cierre de sesión (formato UTC).
  - ☐ Acciones ejecutadas (CRUD, consultas, descargas, modificaciones).
- ☐ Cada evento quedará almacenado con un UUID único para trazabilidad.

Integridad y confidencialidad:

- ☐ Los registros se almacenarán en una tabla de auditoría independiente.
- ☐ El contenido del registro será cifrado.
- ☐ Se garantizará la integridad con un hash por registro.
- ☐ El acceso a la tabla de auditoría quedará restringido por roles, solo para administradores de seguridad.

Transparencia y control:

- ☐ El sistema generará bitácoras inmutables que no podrán ser editadas ni borradas por usuarios comunes.
- ☐ Las modificaciones o eliminaciones de registros estarán bloqueadas a nivel de base de datos.
- ☐ Se habilitará un mecanismo de auditoría forense para reconstrucción de eventos en caso de incidentes.

Revisión y auditoría:

- ☐ El sistema deberá permitir consultas filtradas (por usuario, acción, rango de fechas).
- ☐ Se generarán reportes automáticos en PDF o CSV para el administrador de seguridad.
- ☐ La revisión mínima será trimestral, aunque el administrador podrá ejecutar análisis en cualquier momento.

Roles y responsabilidades:

- ☐ Usuarios: Sus acciones quedarán registradas automáticamente.
- ☐ Administrador de seguridad: Encargado de la revisión y gestión de alertas.

“

Caso 3

Dr. Morales
CONTEXTO COMUNICATIVO 1
El Dr. Juan Morales, médico de emergencias en la ambulancia de la Clínica Médica “SUD”, comparte sus
desafíos con el sistema de gestión de historias clínicas. Acceder a través de la web se convierte en un
problema, especialmente en situaciones urgentes.

""“Cada vez que necesito acceder a historias clínicas mientras estamos en la ambulancia, enfrento dificultades con la versión web. En situaciones de emergencia, el tiempo es esencial, y la lentitud del acceso puede marcar la diferencia. Sería ideal contar con una versión móvil que nos permita revisar la información de manera rápida y eficiente, directamente desde nuestros dispositivos en el campo."
“En emergencias, cada minuto cuenta. Poder acceder a la información de forma inmediata y sin obstáculos es crucial para proporcionar la mejor atención posible. Una versión móvil nos permitiría ser más ágiles y eficientes, asegurando que tengamos toda la información necesaria al alcance de nuestras manos, literalmente."

REQUERIMIENTO

“Considerar el desarrollo de una versión móvil del sistema para garantizar un acceso conveniente y seguro desde dispositivos móviles. Esto facilitará la atención médica remota o en movimiento.”

Cotejo

Lista de cotejo para revisar el requerimiento de la versión móvil

Empleá la lista de cotejo para distinguir entre lo que proporciona información ("Sí") y lo que está ausente ("No") del siguiente requerimiento:

Considerar el desarrollo de una versión móvil del sistema para garantizar un acceso conveniente y seguro desde dispositivos móviles. Esto facilitará la atención médica remota o en movimiento.

✓ Especificación clara de las medidas de seguridad implementadas para garantizar un acceso seguro desde dispositivos móviles: *

- ○ Sí
- ◉ No ✓

✓ Detalles técnicos específicos del desarrollo de la versión móvil: *

- ○ Sí
- ◉ No ✓

✓ Roles y responsabilidades específicos en relación con el mantenimiento y actualización de la versión móvil: *

- ○ Sí
- ◉ No ✓

✓ Información sobre la interoperabilidad con otros sistemas o dispositivos utilizados en atención médica remota: *

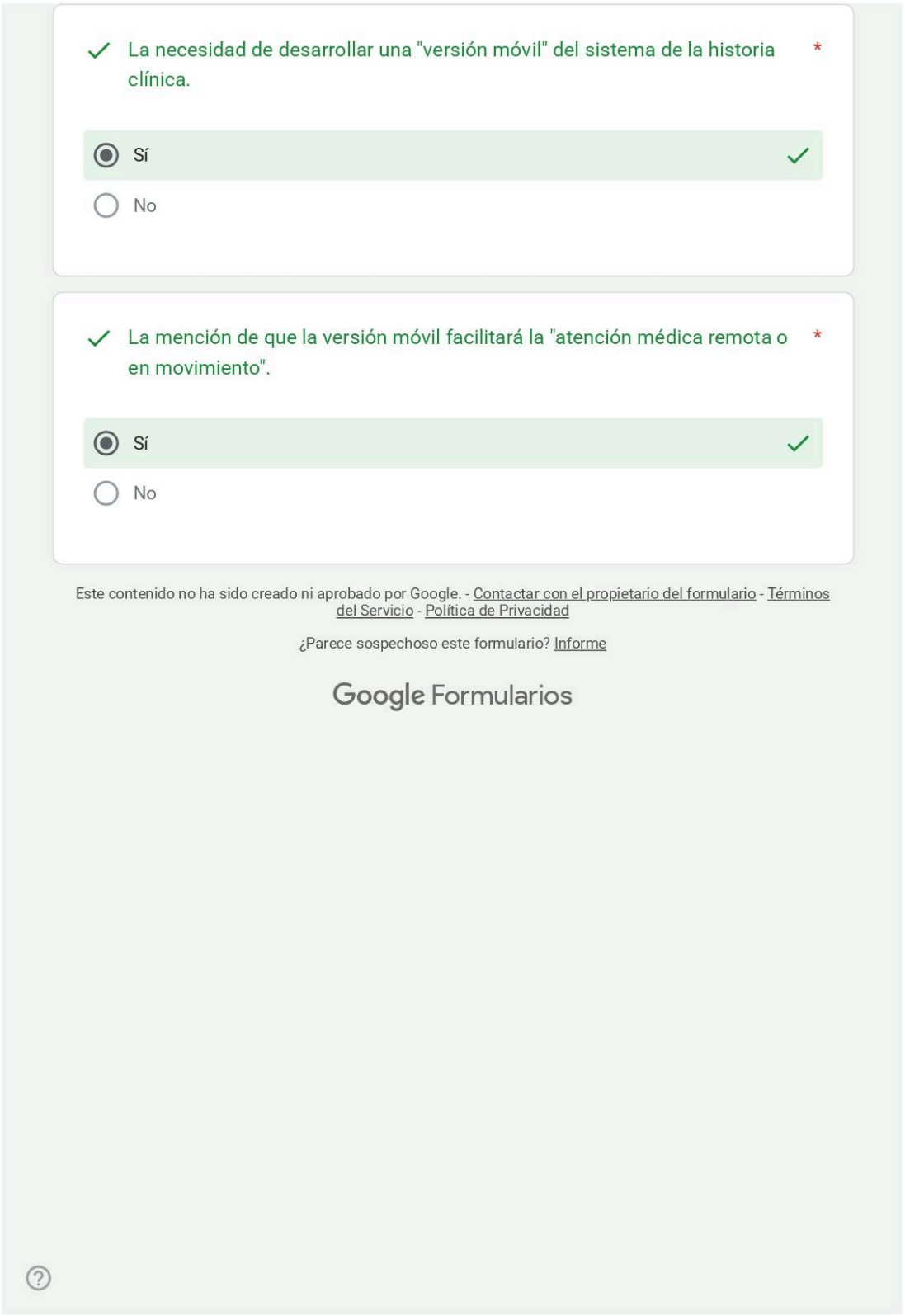
- ○ Sí
- ◉ No ✓

✓ El objetivo de garantizar un "acceso conveniente y seguro" desde dispositivos móviles. *

- ◉ Sí ✓
- ○ No

✓ Detalles sobre la compatibilidad con diversas plataformas móviles (iOS, Android, etc.): *

- ○ Sí
- ◉ No ✓



Requerimiento reformulado

“El sistema de gestión de historias clínicas deberá contar con una versión móvil que permita un acceso conveniente, ágil y seguro desde dispositivos móviles. Esta implementación facilitará la atención médica en movimiento, especialmente en contextos de emergencias o consultas remotas.

- ☐ Versión móvil:
  - ☐ Se desarrollará una aplicación móvil nativa para Android.
  - ☐ La aplicación permitirá acceso completo a las funcionalidades críticas del sistema (visualización de historias clínicas, registro de atenciones, consulta de antecedentes).
  - ☐ La interfaz será optimizada para dispositivos móviles, priorizando rapidez y usabilidad.

- ☐ Seguridad en el acceso:
  - ☐ La aplicación implementará doble autenticación para el ingreso.
  - ☐ Todo el tráfico entre la aplicación y el servidor será cifrado con HTTPS
  - ☐ Los datos sensibles se almacenarán en caché solo en memoria volátil, no se guardarán en almacenamiento persistente del dispositivo.

- ☐ Compatibilidad e interoperabilidad:
  - ☐ La aplicación deberá integrarse con el sistema web ya existente mediante APIs REST seguras.
  - ☐ Será compatible con servicios de terceros usados en atención médica remota.
  - ☐ El diseño será responsivo para adaptarse a distintos tamaños de pantalla (móvil y tablet).

- ☐ Actualización y mantenimiento:
  - ☐ Se establecerá un ciclo de actualizaciones periódicas en tiendas oficiales (App Store, Google Play).
  - ☐ El equipo de TI de la clíica será responsable del mantenimiento, parches de seguridad y mejoras.
  - ☐ Se habilitará un mecanismo de notificación automática dentro de la app para avisar a los usuarios sobre nuevas versiones obligatorias.

- ☐ Transparencia y confiabilidad:
  - ☐ El acceso móvil debe garantizar la misma trazabilidad y auditoría que el sistema web, registrando quién accede, cuándo y qué acciones realiza.
  - ☐ La versión móvil permitirá generar reportes básicos en PDF/CSV para uso inmediato en campo.

“

Registro de la 2.ª actividad seleccionada:

Número y nombre de la sala:	Sala 4 “Requerimientos decodificados”
¿Es de Cámara o de Acción?:	Acción
Nombre de la actividad:	Preguntar para solicitar

Documentación de arquitectura del sistema

de Eduardo Moreno - domingo, 14 de septiembre de 2025, 22:15
Número de respuestas: 0
Les dejo mis 5 preguntas:

1. ¿Qué tipo de comunicación se establece entre los usuarios y el servidor encargado del procesamiento de las solicitudes?
2. ¿Cuál es el componente responsable de almacenar de forma persistente la información clínica de los pacientes?
3. ¿Mediante qué tecnologías se construye la capa visual con la que interactúan los profesionales médicos?
4. ¿Qué medidas se consideran para asegurar la disponibilidad de los datos ante posibles fallos del sistema?
5. ¿Cómo se prevé la interacción del sistema con entidades externas, como laboratorios o instituciones de salud?

Y las otras 2:

1. ¿Qué mecanismos específicos de autenticación y autorización se implementan para garantizar que solo el personal autorizado acceda a las historias clínicas?
2. ¿Con qué frecuencia se realizan las copias de seguridad y dónde se almacenan para garantizar la recuperación ante desastres?

Re: Documentación de arquitectura del sistema

de Eduardo Moreno - domingo, 14 de septiembre de 2025, 22:23
Te dejo mis respuestas :

1. Busca ofrecer una plataforma robusta, segura y eficiente para la gestión centralizada de historias clínicas

2. Los componentes principales del sistema son Servidor de base de datos,Servidor de aplicaciones,Interfaz de usuario

3. Los usuarios interactúan con el sistema mediante una interfaz web basada en tecnologías estándar como HTML, CSS y JavaScript

4. Los servidores de seguridad tienen la función crítica de proteger la información sensible de los pacientes

5. El sistema de gestión de base de datos relacional sirve para Organizar estructuralmente,Permitir consultas eficientes,Garantizar la consistencia, integridad referencial y atomicidad.

Y las otras dos:

1. No especifica ninguna estrategia de escalabilidad pero podria hacerse Particionado de bases de datos, Arquitecturas distribuidas o nube.

2. El documento menciona un sistema de respaldo, pero no habla de que tipo del servicio pero podria ser Si se usa un centro de datos secundario o nube, o Si existen sistemas de alimentación ininterrumpida

Sala 1

Registro de la 3.ª actividad seleccionada:

Número y nombre de la sala:	Sala 1
¿Es de Cámara o de Acción?:	Cámara
Nombre de la actividad:	Planificar para comunicar

¿Por qué elegiste esta actividad? ¿Qué te llamó la atención?

Elegí esta actividad porque me enfrentó a situaciones hipotéticas similares a las que afronto diariamente en mi entorno laboral. Me llamó la atención especialmente por la posibilidad de simular distintos escenarios, algo que me resulta particularmente interesante.

Resolución:

Si estoy liderando un equipo y tengo que planificar el inicio de un proyecto, lo ordenaría de la siguiente manera:

1) Orden de las tareas
   A. Identificar a todos los interesados del proyecto.
   B. Identificar las necesidades desde el principio y transmitirlas.
   C. Preparar adecuadamente la reunión de arranque (Kick Off).

D. Tener en cuenta las habilidades no técnicas para una comunicación fluida.
E. Involucrar a colaboradores en una misma aplicación.
F. Utilizar sistemas de notificación inmediata.

2) Justificación del orden

A. Identificar a todos los interesados del proyecto
Criterio: recursos humanos.
Antes de hablar de requisitos, reuniones o herramientas, necesito saber quiénes son los recursos humanos disponibles (clientes, usuarios finales, desarrolladores, QA, gerencia, soporte, etc.). Sin un mapa de interesados, corro el riesgo de dejar fuera voces importantes.

B. Identificar las necesidades desde el principio y transmitirlas
Criterio: visión y alcance.
Una vez que sé quiénes participan, tendría que levantar requisitos iniciales y documentar qué se espera del proyecto. Esto permite definir objetivos claros y reducir malentendidos más adelante.

C. Preparar adecuadamente la reunión de arranque (Kick Off)
Criterio: alineación del equipo.
El Kick Off es la oportunidad de ver las expectativas, presentar objetivos, roles, tiempos y metodología de trabajo.

D. Tener en cuenta las habilidades no técnicas para una comunicación fluida
Criterio: cultura y clima de trabajo.
La comunicación efectiva evita conflictos y malentendidos. Acá aplico empatía, escuchar y claridad del mensaje, reforzando la dinámica del equipo.

E. Involucrar a colaboradores en una misma aplicación
Criterio: colaboración técnica.
Una vez que el equipo sabe qué vamos a hacer y cómo, puedo organizar la colaboración en el entorno de desarrollo: repositorios, branches, acceso a documentación y diseño de la arquitectura inicial.

F. Utilizar sistemas de notificación inmediata
Criterio: herramientas.
Las notificaciones con herramientas como Slack, Teams, Discord, etc. Se vuelven útiles cuando ya hay dinámica de trabajo. No es lo primero a definir, porque antes necesito a las personas, las necesidades y la forma de trabajo.

Registro de la 4.ª actividad seleccionada:

Número y nombre de la sala:	Sala 1
¿Es de Cámara o de Acción?:	Acción
Nombre de la actividad:	Analizar para mejorar

Situación laboral:
Un desarrollador está trabajando en el frontend de una aplicación y detecta que la API devuelve datos inconsistentes en algunas respuestas. Piensa que su líder técnico ya está al tanto del problema y decide no decir nada.

Interpretaciones:
El resto del equipo asume que "todo está funcionando bien" porque nadie reporta fallas. Días después, el bug llega a producción y afecta a los usuarios finales, generando tickets de soporte y pérdida de confianza en el equipo.

El silencio del desarrollador fue en sí mismo un mensaje: los demás interpretaron que no había problemas. En realidad, su omisión comunicó (de manera no verbal) que todo estaba bajo control. Como en toda comunicación, incluso la falta de palabras transmite información, y en este caso tuvo consecuencias negativas en el proyecto.

Justificación de la elección:
Elegí este axioma porque en un entorno de desarrollo web, donde se trabaja con entregas rápidas, bugs y releases continuas, no reportar un error es tan comunicativo como hablar. El silencio puede ser interpretado erróneamente como "todo está bien", cuando en realidad es un problema grave. Reconocer este axioma ayuda a fomentar una cultura de transparencia, donde se entiende que callar también comunica, y que la omisión puede escalar en fallas más grandes.